NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 35

Best Practices in Computer Network Defense: Incident Detection and Response

Edited by
Melissa E. Hathaway

IOS Press

NATO OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

BEST PRACTICES IN COMPUTER NETWORK DEFENSE: INCIDENT DETECTION AND RESPONSE

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Emerging Security Challenges Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series D: Information and Communication Security – Vol. 35
ISSN 1874-6268 (print)
ISSN 1879-8292 (online)

Best Practices in Computer Network Defense: Incident Detection and Response

Edited by

Melissa E. Hathaway

Global Cyber Security Center (GCSEC)
Rome, Italy

IOS Press

Amsterdam • Berlin • Tokyo • Washington, DC

Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Research Workshop on Best Practices for Computer Network Defense: Incident Detection and Response
Geneva, Switzerland
11–13 September 2013

ISBN 978-1-61499-371-1 (print)
ISBN 978-1-61499-372-8 (online)
Library of Congress Control Number: 2013957833

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

Foreword

Malicious cyber activities are an emerging security challenge for all countries, and the members of the North Atlantic Treaty Organization (NATO) share a responsibility to help the global community strengthen its cyber defenses. One of NATO's unique strengths lies in its ability to tap into the operational capabilities and expertise of its members' militaries, and to harness the innovations and technologies of its members' industrial base to ensure national and Euro-Atlantic prosperity, security, and stability. This commitment was reinforced in the Chicago Summit Declaration of May 2012 when NATO members agreed to address cyber threats to improve their common security. [1]

NATO seeks ways to jointly research, develop, implement, and field interoperable cyber defense capabilities to enhance the cyber defense posture of the Alliance. The NATO Communications and Information Agency (NCIA) is instrumental in meeting this challenge. The NCIA is implementing the best of the capabilities used by its member states and transforming the NATO operating model toward being 'services based.' Cyber defense is being consolidated into one portfolio and cyber services will be offered in a catalogue of services from early 2014. This allows NATO to fulfill some of the requirements outlined in the cyber defense policy by broadening the pooling and sharing of more information on defense technologies, intelligence, and best practices.

NATO is also engaging its network of partnerships, which includes one-third of the world's countries, by facilitating cooperation between all stakeholders—public and private, state and non-state, civilian and military—to reduce the vulnerabilities of national critical infrastructures and achieve a minimum level of cyber defense. NATO recognizes that the more alike each country's approach is, the greater protection we all will enjoy.

NATO Science for Peace and Security (SPS) Programme is an excellent mechanism for NATO's members and partners to share effective practices and solutions for emerging security challenges like those presented by malicious cyber threats. The Advanced Research Workshop (ARW) entitled, 'Best Practices in Computer Network Defense (CND): Incident Detection & Response' generated actionable information that will inform NATO cyber defense policy for the foreseeable future. It identified the state-of-the art tools and processes being used for cyber defense and highlighted our technology gaps. It presented industry and government best practices for incident detection and response, and examined indicators and metrics to measure our maturity along that security continuum.

Our security relies on assurances that our defenses—local, global, procedural, political, and technological—are leading edge and address effectively the threats these services face. These defenses are tested routinely, and cannot fail. We believe that this book will provide operators and decision makers with genuine tools and expert advice for computer network defense, incident detection and incident response. It is our hope that the twenty-one findings from the workshop and the technical papers that underpin those insights will serve to strengthen the cyber defenses of the global community.

Mr. Koen Gijsbers
General Manager, NATO Communications and Information Agency
November 2013

References

[1] Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, 2012. *Chicago Summit Declaration*, para. 49. [online] Available at: <http://www.nato.int/cps/en/SID-D03EFAB6-46AC90F8/natolive/official_texts_87593.htm?selectedLocale=en> [Accessed 15 November 2013].


GLOBAL
CYBER SECURITY
CENTER


GCSP
Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik
Impartial, Inclusive, Influential

Preface

MELISSA E. HATHAWAY
Chairman of the Council of Experts, Global Cyber Security Center (GCSEC)

The Advanced Research Workshop (ARW) entitled, 'Best Practices in Computer Network Defense (CND): Incident Detection & Response' was held from 11–13 September 2013 in Geneva, Switzerland. It was co-sponsored by the Global Cyber Security Center (GCSEC)[1] and the Geneva Centre for Security Policy (GCSP) [2] to explore common interest issues for improving North Atlantic Treaty Organization (NATO) member states' and partners' cyber defense posture. The workshop was enabled by NATO's Science for Peace and Security (SPS) Program and focused on SPS's key priority areas for cyber defense as well as NATO's cyber defense policy implementation [3].

A multi-disciplinary team of experts from sixteen countries and three international institutions gathered to share experience, knowledge, and positions. Together they generated twenty-one specific findings and twelve papers to help improve the cyber defense posture of NATO member states and their partners.

This report contains actionable information and presents examples that can inform decisions. Of the many findings, five stood apart from the others.

First, no organization should accept the status quo. Our networks are compromised and we have become accustomed to assuming that the adversary has penetrated our defenses. Because of this, many organizations have shifted their security approach toward monitoring and detection. Organizations are monitoring ingress and egress routes, and cataloguing the tactics, techniques, and procedures of their adversaries to understand impact and adversaries alike. New tactics and countermeasures are available to strengthen security postures and become more resistant to cyber threats.

Second, commercial entities are developing, deploying, and operating advanced techniques for network defense. The technologies are accessible and affordable, and they are showing promising results. Techniques range from using moving target architectures to confuse the adversary to turning to the Internet Service Providers and Telecommunications Providers to provide an upstream or forward deployed defense. Other effective techniques include monitoring the dark space of the Internet. Intelligence from upstream dark space monitoring can be used to reprogram deep-packet inspection (DPI) sensors within the enterprise zone to detect zero-day activity.

Third, identifying critical services is more important than identifying critical infrastructures. Services, like electric power, navigation, and telecommunications, transcend national boundaries. Changing the focus from critical infrastructure to critical service may change NATO's approach to protection, resilience, recovery, and restoration of assets. It may also highlight the interdependencies between organizations and nations requiring different approaches to common defense.

Fourth, a baseline assessment enables an organization to identify the current state of the controls it has in place to protect infrastructures, assets, and services. Once a baseline is established, it is possible to prioritize a list of the controls that would have the greatest impact in improving risk posture against real-world threats and then map

progress along the path toward a future state that is more resistant, resilient and recoverable.

Fifth, as we continue to invest in digitizing our infrastructure and everything behind it, security considerations must become a core, non-negotiable component of purchasing and acquisition decisions. Work factor analysis can help acquisition and procurement officials determine whether the vendor's product or service will increase the costs for the adversary.

In a domain where speed is essential, where advanced defense is required against advanced offense, and where collaboration and learning amongst defenders are vital, keeping pace and deploying advanced processes or technology is only possible when you know what is available. Knowing what is possible and available, however, and doing something with that knowledge, are quite different propositions – and the latter is in the hands of the reader.

References

[1] The Global Cyber Security Centre (GCSEC) is a global foundation established in 2010. GCSEC is also known as the 'Centro Internazionale per la Sicurezza Informatica.' The Center is enabled by Poste Italiane S.p.A. with the purpose to carry out and promote study, research, teaching, and training for the benefit of society as a whole and organize projects and events regarding the issue of cyber security.

[2] The Global Centre for Security Policy (GCSP) is an international foundation established in 1995 with over 40 member states for the primary purpose of promoting the building and maintenance of peace, security, and stability through training, research, and dialogue.

[3] The new NATO Policy on Cyber Defense provides a solid foundation from which Allies can take work forward on cyber security. The document clarifies both NATO's priorities and NATO's efforts in cyber defense – including which networks to protect and the way this can be achieved.

About the Authors

Sandro Gaycken is a Technology Researcher and a former hacktivist with a focus on cyber warfare. He has been the lead author of Germany's foreign policy strategy on cyber security and Internet freedom. He serves as a regular strategic advisor to governments in Europe and the Middle East, to multinational organizations such as the EU, NATO, and the United Nations, and to legitimate businessmen from Germany's DAX 30 companies. Additionally, he is an Associate Fellow at Oxford University's Martin School for his expertise in cyber warfare and a director in NATO's SPS program on national cyber defence strategies. He does not believe in conventional information technology security and is a strong advocate of disruptive innovation and disruptive regulation.

Melissa E. Hathaway is President of Hathaway Global Strategies, LLC and a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She also serves as the Chairman of the Council of Experts for the Global Cyber Security Center. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. Previously, Ms. Hathaway was a Principal with Booz Allen & Hamilton, Inc., where she led two primary business units: information operations and long range strategy and policy support, supporting key offices within the Department of Defense and the Intelligence Community. Earlier in her career she worked with Evidence Based Research, Inc. and the American Foreign Service Association. Ms. Hathaway has a B.A. degree from The American University in Washington, D.C. She has also completed graduate studies in international economics and technology transfer policy and is a graduate of the U.S. Armed Forces Staff College, with a special certificate in Information Operations.

Elly Van den Heuvel is the Head of the Dutch National Cyber Security Centre (NCSC). The NCSC became operational on 1 January 2012. Its mission is to help increase the resilience of Dutch society in the digital domain and, by doing so, help to create a safe, open, and stable information society. The NCSC is a Public-Private Partnership. Van den Heuvel is one of the principle advocates of this concept. From 2008 till the opening of the NCSC, she was the General Manager of GOVCERT.nl. Govcert is completely embedded in the NCSC. Ms. Van den Heuvel also serves as the Deputy Director for Cyber Security at the National Coordinator Counter Terrorism and Security of the Ministry of Security and Justice. She believes in the power of people who work together for a common goal.

Matthew Holt is the Chief Executive Officer of Intellium. He has more than 23 years of international experience focused on developing national and corporate cyber security strategy, policy, and governance models. His work with both public and private sector clients includes the United States Department of Defense, national and multinational government bodies in Europe and the Middle East, and multiple Fortune 500

companies worldwide. Earlier in his career, he worked for Booz & Company, where he developed the firm's Cyber Security and ICT Resilience service offering, and had ten years of active duty in the United States Air Force as a network engineering and deployment program manager. Matthew currently holds several cyber security certifications including CISSP, CISM, ISO 27001 Lead Auditor, and BS25999 Lead Auditor.

Gerben Klein Baltink serves as the Secretary of the newly established National Cyber Security Council, an independent top-level advisory board for the Dutch Government and Dutch industry. In early 2011 he established his own consultancy firm, focussing on issues of national security, with a small number of employees. Earlier in his career he joined TNO (the Netherlands Organization for Applied Scientific Research) in 1994 and held several positions as junior and senior manager within the Physics and Electronics Laboratory and the Prins Maurits Laboratory. He was Director of TNO Physics and Electronics Laboratory until the 2005 reorganization, resulting in TNO Defence, Security and Safety. He is an active reserve army officer. He completed training at the Royal Military Academy and fulfilled several functions within the 1st Army Corps. He was involved in the reorganization of the Dutch Army in 1991-1994.

Olaf Kruidhof is the Chief Design Authority for the Public Sector and a Principal Enterprise Architect at Capgemini. Before rejoining Capgemini he worked at NATO as the deputy to the Chief Architect and as Group Head of Enterprise Architecture at the NATO C3 Agency, where he was one of the writers of the NATO Network Enabled Capabilities Feasibility Study and worked with the International Military Staff on architectures to implement this strategy. Previously, Mr. Kruidhof worked at Capgemini where he conducted multiple projects, amongst others, for NATO and the Dutch Ministry of Defense.

Felix 'FX' Lindner is the Founder, Technical and Research Head of Recurity Labs GmbH, Berlin, Germany; a high-end security consulting and research team, specializing in code analysis and design of secure systems and protocols. Well-known within the computer security community, he has presented his research for over a decade at conferences worldwide.

Gustav Lindstrom is the head of the Emerging Security Challenges Programme at the Geneva Centre for Security Policy (GCSP). Previously, he headed the GCSP's Euro-Atlantic Security Programme and was the Director of the European Training Course. He currently represents the GCSP on the Executive Academic Board of the European Security and Defence College and serves as co-chair of the Partnership for Peace-Consortium working group on Emerging Security Challenges. Prior to his tenure at the GCSP, Dr Lindstrom served as a Senior Research Fellow at the EU Institute for Security Studies. His areas of expertise include European Common Security and Defense Policy, non-proliferation and disarmament, and cyber security.

David McMahon is the Chief Operating Officer at SecDev Group, where he is working at the intersection of cyberspace, social and political change, conflict, and armed violence. He formerly led complex security programs and research and

development at Bell Canada. With more than 30 years' experience with the military, intelligence, and security community, he has been engaged in the spectrum of operations from special-force, influence-activities, counter-terrorism/radicalization, information warfare, counter-espionage, foreign intelligence. He is a graduate the Royal Military College of Canada in computer engineering.

William Pelgrin is the President and CEO of the Center for Internet Security. He is devoted to improving our collective cyber security. He founded and chairs the Multi-State Information Sharing and Analysis Center (ISAC), a key cyber resource for the United States' state, local, tribal, and territorial governments. He served three terms as chair of the National Council of ISACs. He was appointed to the Commission on Cyber Security to Brief the 44th President, and is currently serving as a member of the State, Local, Tribal, and Private Sector Policy Advisory Committee to advise the President of the United States on all matters concerning the policies relating to access to and safeguarding of classified national security information by U.S. State, Local, Tribal, and Private Sector Entities.

Steve Purser is the Head of the Core Operations Department at the European Union Network and Information Security Agency (ENISA), where he is responsible for all operational activities of the Agency. Prior to joining ENISA, he held various positions including, software developer, project manager, and consultant. From 1993 to 2008, he occupied the role of Chief Information Security Officer for a number of international companies in the financial sector. He was a co-founder of the 'Club de Securité des Systèmes Informatiques au Luxembourg' (CLUSSIL) and has frequently published articles in the specialised press. He is also the author of 'A Practical Guide to Managing Information Security' (Artech House, 2004). Mr. Purser is currently a member of several Steering Boards and Advisory Committees, including notably the Steering Board of the CERT EU and the Programme Board of the EU Cyber Crime Centre. In the area of standards, he is the ENISA representative on the ISO SC 27 working group. As Head of the Core Operations Department, he regularly represents ENISA in international conferences on information security.

Andrea Rigoni is the Director General of the Global Cyber Security Center, a non-profit organization based in Rome, Italy focused on Cyber Security. In addition, he serves as an advisor to the CEO of Poste Italiane on its digital strategy. Recently, he was asked to support the Office of Prime Minister in Italy, participating on a special task force created by the Prime Minister to define the Digital Agenda for Italy and its security. He brings his expertise to many international organizations including the International Telecommunications Union, the PIAC Board at ISACA, and the ICANN review team of the security, stability and resilience of the domain name system. Earlier in his career he worked at Booz & Company as a Senior Associate leading cyber security projects in Europe and Middle East and providing independent consultancy to national governments, international institutions and critical infrastructures. Prior to that, he worked for Symantec in United Kingdom and Middle East and Getronics.

John N. Stewart is a Senior Vice President and Chief Security Officer at Cisco Systems, Inc. He and his team have a three-part mission focused on threat and

response: protect Cisco, protect Cisco's products, and protect Cisco's customers. His leadership at Cisco includes forming the Cisco Security Incident Response Team, the Trustworthy Systems and Cisco Secure Development Lifecycle, and the Security Operations Center. Throughout his 25-year career, he has led or participated in security initiatives ranging from elementary school information technology design to national security programs. Today, he sits on technical advisory boards for RedSeal Networks and Nok Nok Labs, is a special advisor to Koolspan’s Board of Directors, and is on the Board of Directors for Fixmo, Inc., and the National Cyber-Forensics Training Alliance. Additionally, Stewart serves on the Council of Experts for the Global Cyber Security Center and the Cybersecurity Think Tank at University of Maryland University College.

Acknowledgements

The success of the *Best Practices in Computer Network Defense (CND): Incident Detection and Response* workshop and book is due to all of those who participated, including:

John Bassett, Fellow for Cyber Security at the Royal United Services Institute, Whitehall, London and a director of Dianoia Consulting Ltd, United Kingdom.

Laura Crespo, Political Affairs Officer, Division for Security Policy, International Security, the Swiss Federal Department of Foreign Affairs (FDFA), Switzerland.

Cédric Gaudard, Center for Electronic Operations, Swiss Armed Forces, Switzerland.

Sandro Gaycken, Ph.D., Technology Researcher, Computer Science, Freie University of Berlin, Germany.

Melissa E. Hathaway, Chairman of the Global Cyber Security Center Council of Experts, Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, and President of Hathaway Global Strategies, the State of Virginia, the United States of America.

Michael Hausding, Security Engineer, SWITCH, Switzerland.

Marc Henauer, Head of MELANI Operation and Information Center, Bern, Switzerland.

Elly van den Heuvel, Head of the Dutch National Cyber Security Centre (NCSC), Deputy Director Cyber Security (DCS) the National Coordinator Counter Terrorism and Security of the Ministry of Security and Justice, The Hague, The Netherlands.

Matthew Holt, Chief Executive Officer of Intellium, London, United Kingdom.

Heli-Tiirmaa-Klaar, Cyber Security Advisor, Security Policy and Conflict Prevention Directorate, European External Action Service, the European Union, Brussels, Belgium.

Gerben Klein Baltink, Secretary of the National Cyber Security Council, an independent top-level advisory board to the Dutch Government and Industry, Director of KBBa, an Independent Security Consultancy Firm, The Netherlands.

Olaf Kruidhof, Principal Enterprise Architect, Design Authority – Sector Public, Capgemini, The Netherlands.

Martti Lehto, Ph.D., Researcher, Department of Mathematical Information Technology, University of Jyväskylä, Finland.

Felix 'FX' Lindner, Founder, Technical and Research Head of Recurity Labs GmbH, Berlin, Germany**.**

Gustav Lindstrom, Head of the Emerging Security Challenges Programme at the Geneva Centre for Security Policy (GCSP), Geneva, Switzerland.

Kathy Macdonald, M.O.M., Security Consultant, Global Cyber Security Courses (GCSC) Inc., Calgary, Canada.

Pawel Machalski, Cyber Defence Officer, Coordination and Support Centre, Emerging Security Challenges Division, NATO HQ, Brussels, Belgium.

John C. Mallery, Research Scientist, Computer Science & Artificial Intelligence Laboratory, Massachusetts Institute of Technology (MIT), the State of Massachusetts, the United States of America.

David McMahon, Chief Operating Officer at SecDev Group, Ottawa, Canada.

Yoko Nitta, Ph.D., Senior Principal Researcher, Research Institute of Science and Technology for Society, Japan Science and Technology Agency, Tokyo, Japan.

William Pelgrin, President and CEO of the Center for Internet Security; Founder and Chair of the Multi-State Information Sharing and Analysis Center (ISAC) for the United States' state, local, tribal, and territorial governments, the State of New York, the United States of America.

Larry Ponemon, Ph.D., Founder and Chairman, Ponemon Institute, the State of Ohio, the United States of America.

Steve Purser, Head of the Core Operations Department at the European Union Network and Information Security Agency (ENISA), Athens, Greece.

Andrea Rigoni, Director General of the Global Cyber Security Center, Rome, Italy.

Riccardo Sibilia, Head of Cyber Threat Analysis, Command Support Organisation, Center for Electronic Operations, Swiss Armed Forces, Bern, Switzerland.

David Smart, Associate Fellow, Royal United Services Institute for Defence & Security Studies (RUSI), London, United Kingdom.

John N. Stewart, Senior Vice President and Chief Security Officer at Cisco Systems, Inc., Member of the Global Cyber Security Center Council of Experts, the State of California, the United States of America.

Ferenc Suba, Ph.D.,Vice-Chairman of the Board, CERT Hungary, Budapest, Hungary.

Nils Kalstad Svendsen, Ph.D., Head of Norwegian Information Security Laboratory, Giovik University College, Norway.

Katharina Ziolkowski, Senior Analyst, NATO CCD COE, Tallinn, Estonia.

Special gratitude is also owed to **Boriana Maurice** and **Francesca Spidalieri** whose efforts were essential in creating this book.

This page intentionally left blank

Contents

Foreword v
Koen Gijsbers

Preface vii
Melissa E. Hathaway

About the Authors ix

Acknowledgements xiii

About the NATO Cooperative Cyber Defence Centre of Excellence xix

About the Global Cyber Security Center (GCSEC) xx

About the Geneva Centre for Security Policy (GCSP) xxi

Introduction 1
Melissa E. Hathaway

Advanced Research Workshop Findings 3
Melissa E. Hathaway

Computer Network Defense: New Threats and Trends 19
Andrea Rigoni and Gustav Lindstrom

Advanced Technologies/Tactics Techniques, Procedures: Closing the Attack Window, and Thresholds for Reporting and Containment 30
John N. Stewart

Beyond Perimeter Defense: Defense-in-Depth Leveraging Upstream Security 43
Dave McMahon

Back to Basics: Beyond Network Hygiene 54
Felix 'FX' Lindner and Sandro Gaycken

Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities Across NATO 65
Matthew W. Holt

Evolution of National and Corporate CERTs – Trust, the Key Factor 81
Olaf Kruidhof

Standards for Cyber Security 97
Steve Purser

A Model for Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership 107
William Pelgrin

Coordination and Cooperation in Cyber Network Defense: The Dutch Efforts to Prevent and Respond 118
Elly van den Heuvel and Gerben Klein Baltink

Conclusions 130
Melissa E. Hathaway and John N. Stewart

Subject Index 133

Author Index 135

About the NATO Cooperative Cyber Defence Centre of Excellence

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organization, accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently sponsored by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the USA. The Centre is not part of NATO's command or force structure, nor it is funded by NATO, but it is part of a wider framework supporting NATO Command Arrangements.

The NATO CCD COE's mission is to enhance capability, cooperation, and information sharing between NATO, NATO Member States, and NATO's partner countries in the area of cyber defence through of research, education, and consultation. The Centre has taken a NATO-orientated, interdisciplinary approach to its key activities, including: conducting academic research on selected topics relevant to the cyber domain from legal, policy, strategic, doctrinal, and technical perspectives; providing education and training; organizing conferences, workshops, and cyber defence exercises; and offering consultancy upon request.

For information on Centres of Excellence, visit NATO's website 'Centres of Excellence' at http://www.nato.int/cps/en/natolive/topics_68372.htm.

www.ccdcoe.org

About the Global Cyber Security Center (GCSEC)

The Global Cyber Security Center (GCSEC) is a not-for-profit organisation created to advance cyber security in Italy, Europe and around the world.

The Center is based in Rome and was founded by Poste Italiane, together with other leading technological companies. GCSEC aims to develop effective collaboration with Italian and international governmental organisations, industries, research institutes and international institutions.

The mission of the Center is to generate and disseminate knowledge in the field of cyber security in order to create the right conditions for improving cooperation and communication between different stakeholders and for fostering responsive cyber security culture. It also aims to support and advance the development of cyber security capability and skills among organisations and individuals. GCSEC fulfils its mission through the following activities:

- Providing specialised consultancy and support to governmental institutions and businesses on cyber security matters, including drafting political and legal frameworks, shaping national strategies, and implementing national or international security standards;
- Facilitating specialist training and staff development programmes on a wide range of cyber security topics;
- Promoting international cooperation amongst other cyber security centres of excellence for advancing applied research;
- Leveraging the skills and expertise of leading Italian and international experts to facilitate knowledge-sharing and best practice exchange, in order to foster responsive cyber security culture; and
- Supporting government institutions and businesses in their efforts to protect critical infrastructure and critical services.

The Global Cyber Security Center has developed a strong reputation as an international hub for cooperation and innovation. Sharing cyber security knowledge and experience is at the heart of its activities.

www.gcsec.org

About the Geneva Centre for Security Policy (GCSP)

The Geneva Centre for Security Policy (GCSP) is an international foundation with 45 member states which was established in 1995 for the primary purpose of promoting peace, security and stability through training, research and dialogue.

The GCSP is committed to the highest professional standards and trains government officials, diplomats, military officers, international civil servants and NGO staff in relevant fields of international peace and security. Some of the key education and research programmes undertaken by GCSP experts are grouped in the following areas:

- Leadership in Conflict Management;
- Emerging Security Challenges; and
- Regional Capacity Development.

Through research, publications, workshops and conferences the GCSP also provides an internationally recognised forum for dialogue on key security and peace policy issues in the interest of effective security policy decision-making. Some of the latter activities aim to facilitate discreet dialogue in post-conflict situations.

GCSP faculty and senior staff, composed of both academics and practitioners, come from a wide range of countries, disciplines and interests, thus covering a broad spectrum of the peace and security arena. Their acknowledged and extensive contributions to policy and academic debate on global, regional and local peace and security issues include a wide range of books, internationally renowned peer-reviewed journal articles, and other specialised publications, in addition to GCSP Geneva Papers and Policy Papers.

www.gcsp.ch

This page intentionally left blank

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-1

Introduction

Information communications technologies (ICT) and the Internet have been at the forefront of the technological transformation of critical infrastructures, services, militaries, businesses, and society for the last three decades. For the last decade, countries have increased their investments in broad-band initiatives to encourage the adoption and use of new services and capabilities, nurturing the information society into the digital age. Countries are seeing the results of these infrastructure modernization initiatives with enhanced services for e-government, e-banking, e-health, e-learning, e-commerce, next generation power grids, and air traffic control, among others.[1] Yet, this infrastructure-Internet entanglement is a strategic vulnerability that cannot be ignored.

The availability, integrity and resilience of this infrastructure are in harm's way. Sophisticated, malicious cyber actors are penetrating everyone's defenses and most incidents remain undetected for weeks or even months. Traditional defense-in-depth approaches, relying first and foremost on a distinct and hardened network perimeter, have failed. Defensive mechanisms have been outpaced by the scope and scale of offensive innovative techniques and procedures and, as a result, this issue now sits as one of the most important emerging security challenges facing our countries. Defending today's critical information services and infrastructures requires new approaches and advanced techniques that strengthen our collective security and help us prepare for tomorrow's challenges.

The North Atlantic Treaty Organization (NATO) is well positioned to help the global community strengthen its cyber defenses. It has a unique ability to tap into the capacity of its Member States and partner countries to improve capacity for Computer Network Defense (CND) and call attention to effective practices for incident detection and response. NATO's Science for Peace and Security (SPS) Programme is being leveraged to address emerging security challenges like those presented by malicious cyber threats. In September 2013, NATO SPS sponsored an Advanced Research Workshop, entitled 'Best Practices in Computer Network Defense (CND): Incident Detection & Response' to exchange expert knowledge in cyber defense and discuss approaches and solutions to this emerging security challenge. Participants were selected from industry, academia, and public institutions who have direct hands-on experience with and responsibilities for incident detection and response. The workshop highlighted that new tactics and countermeasures are available to strengthen security postures. It further highlighted that commercial entities are developing, deploying, and operating advanced techniques for network defense and that the technologies are accessible, affordable, and showing promising results.

The NATO SPS Programme funded this publication because NATO recognizes that the insights contained within may help the global community become more resistant to cyber threats. This publication begins with the summary of the findings from the workshop. It captures the rich discussion and debate regarding the current state of CND and incident detection and response and highlights the contributions of participants' technical presentations. Twenty-one specific findings are presented and

pathways toward achieving a stronger cyber defense posture are illuminated. Chapter 2 follows with an in-depth analysis of new threats and trends for CND. It describes three ICT trends that present both economic opportunity and potential new vulnerabilities to society. Chapters 3, 4, and 5 identify advanced CND techniques, including state-of-the art tools and processes being used for cyber defense. These three chapters also highlight technology gaps that should be addressed in order to better prepare for tomorrow's challenges. Chapter 6 describes how national cyber security strategies play a key role in shaping a country's approach to CND. It also discusses how overlapping or conflicting requirements imposed by international organizations and individual countries may make national cyber security programs less effective. Chapter 7 describes how Computer Emergency Response Teams (CERTs) are designed and implemented, and discusses the importance of trusted collaboration in effectively handling cyber incidents. Chapter 8 highlights how standards play a key role in improving cyber defense and cyber security across different geographical regions and communities. Chapter 9 discusses how qualitative and quantitative metrics can inform decisions and change behavior. Finally, Chapter 10 highlights a concrete example from The Netherlands of a successful private-public partnership aimed at improving overall cyber security. It shows the reader why effective CND requires close cooperation and collaboration between government and industry, science and education, and national and international efforts.

This publication contains outstanding contributions from internationally recognized experts in the arena of cyber security and cyber defense. Their professional backgrounds and operational experience, combined with their multi-national perspective, provide the reader with deep insights into the state of art and practice of CND, incident detection, and incident response. A more detailed description of their biographies is included at the end of this publication.

This publication contains actionable information to strengthen security and recommendations that, if followed, will help governments take action and reduce risks. In a domain where speed is essential, where advanced defense is required against advanced offense, and where collaboration and learning amongst defenders is essential. Keeping pace with the threat and deploying advanced process or technology is only possible when you know what is available. The information and recommendations in this publication directly support NATO's strategic goal to improve the level of cyber defense within the geographic scope of the Alliance and its partner countries.

The Geneva Centre for Security Policy and the Global Cyber Security Center would like to thank all the authors for their time, expertise, and contribution to this publication. We believe that your work will have enduring impact on the global community.

Ms. Melissa E. Hathaway
Chairman of the Council of Experts, Global Cyber Security Center (GCSEC)
November 2013

References

[1] Hathaway, M. E., 2013. Cyber Readiness Index 1.0. Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at: <http://belfercenter.ksg.harvard.edu/publication/23607/cyber_readiness_index_10.html> [Accessed 15 November 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-3

Advanced Research Workshop Findings

MELISSA E. HATHAWAY
Council of Experts, Global Cyber Security Center (GCSEC)

Introduction

The NATO Science for Peace and Security Programme (SPS) seeks to enhance cooperation and dialogue on emerging security challenges by gathering insights from member states and partner countries, exploring basic and applied research activities, and sharing effective practices of advanced operational activities that are undertaken by private industry and public institutions. SPS initiatives are aligned with North Atlantic Treaty Organization (NATO) strategic objectives.

One emerging security challenge is that every country has embedded Information Communications Technologies (ICT) into every networked infrastructure. These technologies are designed to meet the demands for consumer ease of use, increased interoperability, and enhanced efficiency and productivity. There is increasing recognition that these products and services are not always well engineered and often have vulnerabilities that are being exploited for illicit and illegal purposes. In fact, the defenses of these networked infrastructures are tested daily, and the pace and scale of these threats is increasing in terms of frequency and gravity.

In 2011, NATO adopted a new cyber defense policy that articulated a clear vision of how the Alliance plans to improve its cyber defense posture. NATO understands that it must improve its capacity for Computer Network Defense (CND) and adopt effective practices for incident detection and response, especially with regard to the national networks on which NATO relies to carry out its primary mission of collective defense and crisis management. As such, an Advanced Research Workshop (ARW) entitled, 'Best Practices in Computer Network Defense (CND): Incident Detection and Response' was held from 11-13 September 2013 in Geneva, Switzerland, to exchange expert knowledge in cyber defense and discuss approaches and solutions to this emerging security challenge. Participants were selected from industry, academia, and public institutions which have direct hands-on experience with and responsibilities for incident detection and response. The workshop format included technical presentations followed by facilitated discussion in six key areas:

- What are the new threats and trends challenging operators and decision makers?
- What is the role of national and international strategies, legislation, and regulation to improve national incident response and international coordination?
- What are effective mechanisms for coordination and cooperation to prevent and respond to incidents?
- What emerging technologies exist for advanced prevention, detection, containment, and remediation for computer network defense?
- What metrics exist for measuring cyber security effectiveness?

- What is the role of standards and which standards are proving most useful for CND?

There was rich discussion during the course of the workshop and nearly a dozen technical papers were authored to support the exchange of information on effective policies, strategies, technologies, practices, measures, and standards for CND, incident detection, and response. The following paragraphs capture the essence of the discussion and discuss twenty-one specific findings from the workshop. Each finding contains expert insights, important examples, and actionable information that can inform decisions.

1. Detection has Replaced Defense as a Strategy.

Cyber security incidents are increasing in both scope and scale every day. Intellectual property and personal information are illegally copied, online and critical services are disrupted electronically, systems are erased or destroyed, and sophisticated malicious cyber actors are very active and often remain undetected for quite some time. Our political, military, and corporate leaders are inundated with, and increasingly numb to, the news reports and alerts from network operations centers informing them of yet another incident. The reality is that our networks are compromised and we have become accustomed to assuming that the adversary has penetrated our defenses.

We often assumed that we had a distinct and hardened network perimeter that is not actually there. This assumption led to a false sense of security that we must now address head-on. Many institutions shifted their security approach toward monitoring and detection, as defenses failed. Every 2.2 seconds, new malware is detected, and recent reports indicate that 85 percent of breaches take at least one week to detect. Organizations are monitoring ingress and egress routes, cataloguing the tactics, techniques, and procedures of their adversaries to understand impact and adversaries alike.

There is a concern that leaders and operators are accepting this fait accompli. New tactics and countermeasures are available to strengthen security postures and become more resistant to cyber threats, rather than just detect their success.

2. Advanced, Effective Techniques for Defense are Operating in Industry and Showing Promising Results.

Commercial entities are developing, deploying and operating advanced techniques for network defense. The technologies are accessible and affordable and are showing promising results. The workshop illuminated many examples, only a few of which are highlighted here.

For example, enterprises should not be fixed targets ready to be breached if it is possible to make them moving targets. Data center systems do not ‘change’ much from day to day; the Internet Protocol (IP) addresses, service, machine names, and configurations change infrequently, therefore an adversary can and will study them. Moving target architectures are possible in today’s virtual world. They can be designed to change their configurations, thus introducing confusion for the adversary, creating more difficult environments in which to maintain persistent connections, and increasing

the potential for attack discovery. Using virtualization and virtual machine clusters in data centers, it is possible to reboot at will and/or randomly without interrupting service. This 'start from scratch' approach makes the virtual machine jettison malware if infected, and interrupts any covert, undiscovered activity from continuing on the host. Last, it resets the system baseline, which has the potential to illuminate a re-infection attempt if instrumented to do so. A key element to success in virtualization is Intel Trusted eXecution Technology (TXT) or a similar capability which helps ensure the software and service validity.

Some industry sectors are turning to the Internet Service Providers and Telecommunications Providers to provide an upstream or forward deployed defense. Upstream security is a layer of controls and safeguards beyond the enterprise perimeter. It leverages the perspective on Internet traffic available to telecommunications providers. These providers are unique because their infrastructures and services are where the physical elements of cyberspace (lines, wires, and routers) correlate with traffic flows, content and national and jurisdictional barriers. They are able to bring to bear significant technical capabilities and a perspective on traffic flows to rapidly create a security layer that can potentially operate with higher efficiency and effectiveness then any enterprise security program. The bulk of malicious traffic (toxic content) can be stopped proactively using network traffic analysis, stopping the malicious activity before it reaches an organization by invoking upstream security controls deployed at choke points or cleaning centers.

Another technique being used by industry is monitoring the dark space of the Internet. Think of dark space as the unassigned domains or IP address blocks within the Internet that harbor malicious activities; it is the 'ungoverned' territory of the Internet. Intelligence from upstream dark space monitoring can be used to reprogram deep-packet inspection (DPI) sensors within the enterprise zone to detect zero-day activity. Additionally, traditional security sensors are made aware of the persistent threat, signatures, and blacklists can be generated back, and then web and e-mail filters, routers, intrusion prevention systems and firewalls can be updated to stop the malicious traffic or exfiltration of sensitive materials dead it its tracks.

Without question, mastering IT basics for network security controls is proving effective. Conducting an asset inventory and software service mapping provides a base line assessment of an organization's attack surface. Employing strong identity solutions instead of fixed or complex passwords helps reduce impersonation and illegitimate use of privileges in a system. These activities that help an organization know its own infrastructure are provably reducing the attack surface. Organizations should seek to control what they can and do it well.

3. National Strategies are Rarely Written as Risk/Threat Based, they Outline Organizational Roles and Missions.

A global dialogue on information security emerged in the last decade and at least thirty-five nations have published their cyber security strategy, outlining key steps that are intended to increase the security and resilience of their nation. Common topics in these strategies include: outlining organizational and positional authority within the government; fostering awareness and education among the citizens; building an incident and crisis management response capability; expanding law enforcements capacity to deal with the rate of cyber crimes; facilitating private-public partnerships

and developing trusted information sharing exchanges; engaging in international dialogue on issues such as privacy, security, and data protection; and marshaling resources toward a research and development (R&D) and innovation agenda.

Many strategies begin with statistics, quantifying incident volume, the rate of infrastructure infection, and naming the variety of threats. The data is used to justify organizational responsibility and increased funding for missions and organizations. Rarely do these strategies prioritize which services and infrastructures are most at risk, nor do they align the security measures and resource requirements necessary to reduce exposure.

Current trends indicate that incidents will continue to increase in terms of frequency and gravity for the next three years and the costs both for defense and from their effects will increase quicker than benefits created by online services. A richer risk-based approach that includes deterrence and defense, critical services and protection costs that adapts to a constantly changing environment will better inform national approaches.

4. Threat Assessments Increase Understanding and Document Trend.

Threat assessments document threats, trends, and impacts to infrastructures and essential services. They are written in a manner that helps increase understanding of the situation and give evidence of the threat and risks to society. Often the assessment includes a technical annex that provides more detail on the vulnerabilities, exploits, and technological solutions. In some countries the assessments are produced in collaboration with the private sector and thus provide a broader picture of what the private and public sectors are facing on their infrastructure and networks. The Netherlands, Sweden and Germany are working together to present a combined threat assessment intended to inform a broader set of policymakers and begin to give a northern European assessment of the trends and impacts they collectively face.

5. Closing the Gap between Policy Maker Understanding and Frontline Realities is Essential.

The cyber topic is vast and complex and perhaps no one understands it fully. We are dependent on technology for our day-to-day lives, including civilian and military operations. The mobile phone is the primary means of communication for an increasing proportion of the population and the speed and availability of information provides businesses and militaries with an operational edge over adversaries and competitors.

Yet, industry reports regularly cite facts and figures that show this dependence could be a strategic weakness. National leaders are alarmed at the depth and breadth of intellectual property theft and data leakage. Corporate leaders worry about disruption of service or worse, destruction of property. National threat assessments suggest that the trends and incidents will continue. Despite all of these awareness-raising activities, key decision makers' understanding is still low.

Public and private sector leaders find themselves deciphering technical details regarding threats to technologies that they cannot live without. Network operators and chief information security officers are the front-line defenders. They are battling the armies of infected computers that are using the ubiquitous bandwidth to deliver

payloads against our core services and infrastructures including water, power and telecommunications. There is a new weapon (malware) detected every 2.2 seconds and the arsenal appears limitless.

Policy makers are in a position to change the situation through policy, law, market mechanisms, regulation, standards, and other means at their disposal. Bringing tighter alignment and shared understanding of the operational realities and policy implications is essential to ensure the right decisions are made.

6. Awareness is not Enough; It Should Lead to Informed Action.

Public and government awareness is crucial, but it may not be enough to drive a citizen, an organization, or a nation to action. It is important to describe the situation so that everyone has real, genuine shared needs. For example, if we do not act now, we put at risk electricity or telecommunications continuity and availability. In other words, if a country cannot deliver these essential services, it puts at risk critical services such as heating for housing, telephone services, or food and water. Shared awareness must improve so that every individual who has to act along the decision making chain does so.

International organizations like NATO as well as nations and corporations, have a role to play in creating 'perspectives of action.' The roles range from coordinator, communicator, or consultant to initiator. It is time to embrace current understanding of the situation and dust off or create the action plans and begin execution, and then take informed action.

7. Member States are Establishing Unique Learning and Response Mechanisms.

Most nations are placing cyber defense at a priority equivalent to defending land, sea, air, and space. Some nations recognize that they need to mobilize unique information sharing mechanisms and partnerships to create a network that provides early warnings and a better perspective for action. For example, the Netherlands established a National Defense Network to incubate learning and response mechanisms. They are seeking synergy through combining local activities on a national level. Their credo: incident response at one organization means incident prevention at another organization. The system intends to share information on current threats which have possible high impact across all monitoring systems, processes, and organizations.

Hungary has implemented a similar system and is using a traffic light protocol for sharing classified but confidential information across industry sectors. Norway has developed a unique partnership with academia. For example, the Norwegian Armed Forces are working closely with their research community to develop options to detect hackers and malicious activities. They realize that it is not just about fixing a computer; rather, it is about approaching the operational problem more holistically with more tools from the academic and research community.

8. Political Commitments May be Equally Effective (binding) as Legal Agreements and Treaties.

International fora are becoming the venues where nations debate the merits of formal rules of engagement in cyberspace and the need for international treaties to govern the policy, operations, economics, and standards of the Internet. However, international treaties are signed exclusively between nations' governments, and do not account for the requirements of industry and civil society. While treaties may be legally binding, politically binding agreements may be equally effective (and each may be broken with consequences).

The Internet is a public good, similar to the natural environment of air and water. The natural environment is a concern of humanity. Globally we are trying to limit air pollution and assure that clean drinking water is available. Political agreements regarding cyberspace and the Internet may involve the whole of society as stewards of the Internet environment and thus have broader impact.

9. Member States Are Investing in Disruptive Innovation and Considering Disruptive Regulation.

Some nations have determined that evolutionary defenses are insufficient and are investing in new and disruptive technologies that meet higher security requirements informed by national security requirements (e.g. military). They are coupling this innovation strategy with the necessary market levers to create rewards and punishments. This approach aligns security measures to the risks. Capability building and education initiatives that deliver competitive, secure solutions vis-à-vis the traditional insecure solutions at market price will be rewarded. Disruptive regulation is also being considered to introduce technical standards, certifications, and processes to drive insecure products out of the market place.

10. Regulated/Directed Coordination Rarely Leads to Trusted Information Sharing.

Many countries in Europe, as well as the United States, are trying to codify information sharing in policy, regulation, and law. The initiatives range from specifying the time requirement of breach notification[1] to mandatory sharing of the technique or method used in the penetration to include samples of the malicious software, if discovered and isolated by the organization. Policy documents such as cyber security strategies are also outlining the need to establish a computer incident response capability.

Nations believe that it is necessary to formalize information sharing processes to gain better situational awareness of the threat and trends, enable the timely delivery of threat and impact information (early warning data) to improve defenses of all entities, and increase resilience by reducing cyber risk. These initiatives are running into some problems due to a lack of trust; each party is trying to protect its sensitive data from disclosure. Some entities require protection from the United States' *Freedom of Information Act* (FOIA). Others are classifying the data as confidential or even higher. Each one of these protection mechanisms leads to data that is available but cannot be shared with those who need it. Some nations have established 'traffic-light' protocol to

parse the data and prioritize what can be shared. Other nations have had to codify in law an information-protection program to enhance voluntary information sharing between infrastructure owners and operators and the government.

While formal mechanisms may be necessary, they should not break the informal information sharing environments that exist and are effective. For example, the Forum for Incident Response and Security Teams (FIRST) brings together a variety of computer security incident response teams from governmental, commercial, and educational organizations. It is an informal network that fosters cooperation and coordination in incident prevention, enables rapid reaction to incidents, and promotes information sharing among members and the community at large. The FIRST culture and successes are often brought into other organizational, military, and national Computer Security Incident Response Teams or centers (CSIRTs).

Formal and informal information sharing mechanisms need to operate in parallel, and ideally be mutually re-enforcing. As nations consider regulating information sharing, they should be careful not to break the very mechanisms that are working now.

11. Effective (Best) Practices Exist and are Underused at Organization, Sector, National, and International Levels.

A best practice is a method or technique that has consistently shown results superior to those achieved with other means. It usually becomes a benchmark or standard way of doing things that multiple organizations can use. Effective practices exist at organizational, sector, national and international levels for many things, including interoperability, safety, and security. There are pockets of excellence that could be leveraged to minimize the duplication of effort and maximize security postures. For example, a chief security officer for a large and diverse state government used the Intentional Standards Organization (ISO) controls to increase the security posture of the state. The controls were categorized into four levels of criticality so that organizations could incrementally address: (1) critical defenses; (2) defensive readiness; (3) defensive planning; and (4) security training and awareness. Compulsory timeframes and reporting requirements were established and this approach improved the overall state security posture. It is now being leveraged at a national level.

National guidance is also emerging to facilitate the broader use and application of a technology or a process to promote security. For example, the Australian Government published Strategies to Mitigate Targeted Cyber Intrusions, the British Standards Institute recently published Cyber Security Risk – Governance and Management Specifications, and the European Energy Regulator (ENTSO-E European Network of Transmission System Operators for Electricity), in its Network Code on Operational Security[2] recommends that operators define comprehensive organizational, logistical, and technical plans, with a particular attention to alert, detection, and restoration procedures.

Economies of scale can be achieved if effective practices are published, distributed, and leveraged. An effective exchange of how things are working and what is effective creates a learning environment, increases cooperation, reduces duplication, and leads to a more effective and efficient defense.

12. Formal and Informal Relationships and Networks are Equally Important.

The power and influence that individuals have within organizations, or of organizations and entities within a broader network, cannot be underestimated. Ideas, products, messages and behaviors spread through these networks, connecting us with new information. Trust builds over time based on the value of the connectivity, the contribution to the mission, and the usefulness of the information. For example, the underground economy facilitated through criminal networks is thriving. In general, it is a sketchy, low-trust environment where dishonest people are working together toward a common purpose (to make money) and collectively fear penetration of their network by law enforcement. Their clarity of mission and purpose is clear: exploit cyber space to make money. The cyber defense mission does not enjoy the same level of trust or speed of information sharing. Partly, this is because organizations may be working toward different goals, including protecting data, detecting fraud, or stopping malware from entering the network. Clarifying the purpose of collaboration and information needs can be a driver for effective relationships and networks.

Europol and the European Cyber Crime Center recognize that it is difficult to build trust virtually. They embraced this problem and are connecting each member state's law enforcement and Center of Excellence (CoE) through face-to-face meetings and conferences. As a result, these law enforcement professionals know each other better, have increased trust among themselves and tend to collaborate more easily. The cyber defense community and the national and military CSIRTs would benefit from a similar approach.

Training and exercises are additional tools to build networks and communities and get people and organizations to work together. NATO holds a Cyber Defense Exercise and Crisis Management Exercise annually to test Alliance technical and operational cyber defense capabilities. Expanding these traditional initiatives into other venues may help build NATO's non-traditional networks and enhance its overall cyber defense posture through cooperation with partner countries, organizations, and commercial entities. For example, ENISA holds an annual Cyber Exercise that is establishing baseline mechanisms and procedures for communications between member states for cyber incident contingency planning and recovery. Similar exercises are taking place in the United States and Germany, helping decision makers understand the second and third order effects of cyber incidents.

13. Identifying Critical Services is more Important than Identifying Critical Infrastructures.

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and the economy. The infrastructures include electricity generation, gas and oil production, telecommunications, water supply, transportation, financial services and other essential services. Many nations are focusing on securing these critical infrastructures and protecting critical systems as part of their cyber defense posture. However, the focus is more on the protection of the physical asset and logical function of its components rather than the product or service that it is providing to society.

Defining what is critical to the function and operations of an organization, a nation, and an alliance like NATO may differ. A bottom-up review may only identify assets

within the ambit of the organization or nation, and overlook shared services that transcend borders. For example, assuring the integrity and function of a nuclear power plant may be the sole responsibility of a company or country. A top-down assessment may identify common or transnational assets that are essential to the function and operations of an organization. For example, the undersea channel tunnel between the United Kingdom France, and Belgium is a shared infrastructure that requires shared protection.

Services also transcend national boundaries. When the European Commission asked its member states to identify critical infrastructures (bottom-up), they did not identify important shared assets like the satellite navigation system of *Galileo*. E-commerce, transportation, and many other services are dependent on satellite navigation. If the signals were switched off or failed tomorrow, it would have a wide effect on many critical services of many nations. When services such as this are included in security strategies, it raises questions such as who is responsible, accountable, and ultimately who pays for the security and defense. This is very similar to the debate that is underway about collective defense in NATO.

Changing the focus from critical infrastructure to critical service may change the approach to protection, resilience, recovery and restoration of assets. It may also highlight the interdependencies among organizations and nations requiring different approaches to common defense.

14. A Baseline Assessment is Essential to Measure Current and Future Effectiveness.

A baseline assessment enables an organization to identify the current state of the controls it has in place to protect infrastructures, assets, and services. More often than not, an organization does not know the composition of its enterprise because new technologies, applications, and products are layered onto existing systems. This trend will continue as organizations adopt the next generation technologies and enable employees to 'bring your own device' (BYOD) to work. Therefore it is important to know what comprise an organization's critical services and assets and know the information security and other controls that are in place to manage the risk. Once a baseline is established, it is possible to prioritize a list of the controls that would have the greatest impact in improving risk posture against real-world threats and then map progress along the path toward a future state that is more resistant, resilient, and recoverable.

There are well-established baseline controls that are available to provide an easy checklist to assess where one stands vis-à-vis an established set of criteria that have proven effective in increasing an overall defensive posture. One baseline was established by the SANS Institute: the Top Twenty Critical Security Controls (CSCs).[3] These CSCs were developed through recommendations and consensus among a consortium of international agencies and private industry from around the globe. These controls are effective in countering advanced threats the network and enterprise. The Australian Government developed Strategies to Mitigate Targeted Cyber Intrusions and its controls have proven at least 85% effective in preventing targeted cyber intrusions.

Finally, standards such as the International Standards Organization (ISO) 27001 encourage the adoption of a blueprint for setting up a management system for security

as well as a system for auditing and checking compliance of an organization with security best practices. When put into practice, these security controls can help an organization track trends and patterns and identify areas that require more focused attention. This was done recently in the United States to assist hospitals in assessing their own cyber security readiness, along with ascertaining hospital readiness levels in comparison to others. The assessment was conducted at 109 hospitals and each facility was able to ascertain where it stood vis-à-vis other hospitals and sector leaders. The assessment provided specific guidance through recommended effective security controls, practices, and standards and provided a roadmap for improving each organization's cyber security posture.

Conducting a baseline assessment is an effective practice that should be a part of an organization's standard operations. It was noted that NATO has not conducted a baseline assessment to compare where it is vis-à-vis where it wants to go.

15. Training/Exercising for Crisis Management Situations Builds Relationships, Processes, and Confidence.

An organization's preparedness for crisis management situations can be based on knowing its critical services and dependencies as well as knowing its strengths and weaknesses from the baseline assessment. While no organization wants to experience a crisis, all organizations would benefit from knowing how well they will operate under duress. One way to prepare for this is through training and exercises. For example, the German Executive Branch conducted a one day Crisis Planning/Readiness Exercise in November 2011. The goal of the exercise was to work out procedures for how the government would deal with a multi-pronged attack that included: a Distributed Denial of Service (DDoS) attack against critical infrastructures; insertion of malware into the banking system, causing a crisis with ATMs and credit cards; and insertion of false traffic within the air traffic control system. The crisis forced leaders to work out information flows for decision-making and focused on government processes to include who is in charge during a crisis such as this. It also demonstrated the interdependencies of key services and the downstream effects of cascading failures.

More recently, multi-national exercises force nations and militaries to attempt to carry out their duties with degraded networks. Teams conduct daily assessments and find critical vulnerabilities that would further degrade network architectures. Usually the goal of these exercises is to optimize processes and procedures for NATO or whatever set of nations are working together. It is important to consider that most Internet or cyber activities are global in scope and considering non-partner countries and companies may be necessary to ensure that the networks remain safe and operational. For example, shortly after the establishment of the National Cyber Security Council, the Netherlands was confronted with the DigiNotar crisis. This incident, in which certificates were stolen from a major Dutch registrar, resulted in (initially improvised) close cooperation between government, industry, and the scientific community. The Council became actively involved in discussing the possible actions and necessary coordination between government, business, and society, some of which existed outside of the borders of the Netherlands. Mutual trust was built from the actual experience of cooperation and dialogue. Now, the lessons learned from the incident can be shared with other nations and CSIRTs and its experience acts as a 'wake-up call' for all parties involved.

16. Qualitative and Quantitative Metrics Inform Decisions, Test Hypotheses, and Forecast Future State.

Cyber defense and cyber security are top of mind of many political, military, and corporate leaders. One of the leading priorities is to the reduce threats that exploit common vulnerabilities of organizations' information systems, assets, infrastructures, and people. Regulation and other compliance mechanisms steer our leaders toward a checklist mentality rather than focusing on performance outcomes. Metrics, both qualitative and quantitative, can inform decisions, test hypotheses and help forecast, through trend data, the future state of the organization.

Choosing the right metrics for the right purpose to inform decisions and obtain the right outcome is vital; bad metrics will take you off course. Some leaders focus on qualitative metrics like the legality of an action, or whether an entity is compliant, or more recently, the propriety of actions taken. Others focus on more quantitative and statistical metrics, measuring rate, frequency, tempo, and scale. Examples of these data include number of security incidents or breaches; quantity of malware generated, collected, or analyzed; cost of a data breach; number of stolen devices; loss of intellectual property, time to recover, frequency of outage, quality of service, etc. Industry reports are published regularly and nations publish annual reports to inform our decisions.

Yet it is what leaders do with the data points that matters. If an incident cost is lower than what it may take to counteract it, then it is likely that no action will be taken. Metrics need to be translated into the 'so-what?' or impact. For example, does this event affect reputation, customer or citizen confidence, quality of service, quality of protection, GDP growth, morale, citizen safety, or lives? Metrics need to be used to change behavior and make a difference.

17. There is not Enough Research or Discussion on Recovery and Reconstitution.

Institutions have shifted their security approach toward monitoring and detection, and away from defense, but few are researching or discussing the topics of recovery and reconstitution. The outcome of a cyber incident can be greatly affected by the way the organization manages the situation. The organization must know its critical services, assets, and information. This will help inform how it maintains continuity of operations. Understanding how quickly mission critical services and assets can be restored in the event of an emergency helps to minimize the impact on employees, partners, and customers. For example, knowing whether the enterprise will gracefully degrade or fail catastrophically is important. Knowing the number of hours or days it will take to restore operations to their normal state under different crisis management scenarios is equally important. Of course, the availability of systems is essential to the viability of business, and business continuity plans are part of that process. More research and discussion is required to drive strategic thinking toward pro-active preparation for the restoration of critical services and assets. The research and discussion should inform the planning process and be tested and exercised using different scenarios.

18. Military Specifications Can Raise the Bar on Industry Solutions.

NATO and militaries have a unique position in the market. They can use their purchasing power to influence industry to deliver higher assurance products and services. This can lead to cross-over products that can become leaders in the commercial marketplace. For example, military requirements for all-weather, rugged terrain gear, and products for extreme climates resulted in the development of more resilient camping gear, specialty clothing, kevlar luggage, and special communications equipment. In addition, if you spec for military grade today, it can become commercial grade tomorrow. This was the case for the Internet. It was born from the military requirement to have assured communications in the event of a nuclear war and now it is the backbone of the global economy.

The lack of assurance in commercial products may require special purchasing requirements not currently available. If the military continues its dependency on commercial-off-the-shelf products and services it should ensure that they be measurable, enforceable, useful, and provable.

19. Acquisition, Purchasing, and Security Decisions are not Mutually Reinforcing.

Improving security requires tighter alignment between acquisition, purchasing and security. Each has an important role to play in driving a higher defense and security posture and each can easily overlook its responsibility in the process. For example, in current advanced IT systems such as cloud computing, organizations and users buy capability such as storage, analysis, or file sharing without security being key to the decision. Cloud computing and virtualization technologies offer many benefits and cost savings but they also come with potential information security and assurance pitfalls. Knowing if the cloud provider can ensure the confidentiality, integrity and availability of your information with mature processes, proof of past performance, understanding of and mechanisms for disaster recovery options, and encrypted back-ups is essential.[4] These are just a few of the security requirements that could and should be part of the procurement and acquisition process.

Additionally, there are new methods that can help acquisition and procurement officials evaluate the effectiveness of the proposed product or service through using the lens of a work factor analysis. Work factor analysis aims to evaluate the costs imposed on the attacker and advantages favoring the defender in terms of computational complexity, cost, knowledge, other resources, and risk management. This method helps evaluate how to maximize the impact on the adversary's behavior (e.g., increase their costs, complexity, time to execute) with minimum resources. It also helps ascertain the difficulty associated with executing attack or defense across technical systems as they are deployed within organizations or societal infrastructures. Procurement and acquisition officials then can more easily detect the inadequacies and weaknesses in vendor products and services and demand, if appropriate, stricter requirements. This process of maximizing the costs for the adversary could be embedded in every acquisition.

Another security consideration for acquisitions is to demand smaller building blocks and formal languages for product composition. The smaller the building blocks are, the more communication is required between them. This is desirable because

communication interfaces are where security can be most easily modeled, implemented, and enforced. Some refer to this language-theoretic approach as the 'LangSec' effort. This method builds security at the beginning of the process by examining system and program components as computational automata, both in isolation and when composed into larger systems. It also explores how to employ language-theoretic principles to construct software that is robust by design and exposes as little state and computational power as possible to adversaries.

As we continue to invest in digitizing our infrastructures and everything behind it, security considerations must become a core, non-negotiable component of the purchasing and acquisition decisions.

20. Conflicting and Competing Standards Exist Now and Need Resolution.

Standards have an important role to play in improving approaches to information security across different geographical regions or different communities. Some of the more important reasons include: (1) improving the efficiency and effectiveness of key processes; (2) facilitating systems integration and interoperability; (3) enabling different products or methods to be compared in a meaningful manner; (4) providing a means for users to assess new products or services; (5) structuring the approach to deploying new technologies or business models; (6) simplification of complex environments; and (7) promoting economic growth.

The number of standards development organizations and the number of published standards has increased, especially in the area of information security. Nations are using standards to meet different objectives and in some cases standards are being imposed that are competing and contradictory. For example, in Europe, data protection directives impose strict controls on protecting personal identifiable information. This will directly conflict with the draft Directive on Network and Information Security, which requires organizations to notify authorities of a breach within 24 hours of the event. This will require network defenders to review log information that will contain personal, identifiable information. It is unclear which directive or standard takes precedence. More troubling is the fact that following one, if compelled by regulation, requires an organization or entity to break the law by not following the other. There are other competing standards that conflict or compete with each other for adoption and it is often difficult for the end user to judge which standards are the best choice for their particular requirements.

Standardizing processes and procedures are an essential part of achieving effective cooperation in a cross-border or cross-community environment. Without such standardization, communication is likely to be inefficient and could result in an ineffective process. Some areas where published and adopted standards could help the NATO alliance are: cyber defense training procedures and ranges; exchange of cyber threat intelligence (i.e. a malware information sharing platform (MISP)); and definition of effective practices for the verification of security in national security relevant systems that are not based on the common criteria standard. The development and use of these standards is necessary and timely, and they do not need to be open-standards based.

21. Standards are Only One Way to Improve Security - Not The Way to Improve Security.

Standards are important, but they should be viewed as only one mechanism to improve cyber defense and security. It is important to note that specific issues should be considered. First, using, adopting, and following a set of standards may not lead to a stronger defense or higher security posture. Some organizations may use standards for standards' sake, meeting a set of compliance requirements or to check-the-box that they are following a particular process. This may lead to a false sense of security or, worse yet, make the organization less secure.

Second, designing and agreeing to standards is a lengthy process, usually measured in months (in the best cases) or years. Because the process is so long, it does not keep pace with the technology lifecycle. Therefore, it may be important to impose a time efficient process like a 'fast-track' mechanism to help create agility and fulfill the purpose of using the standard in the first place. Additionally, newly selected standards must increase ease of use and assure higher security and not help the adversary.

Finally, standards do not replace common sense or creative thinking. Standards are tailored compliance mechanisms and steer leaders toward a checklist mentality rather than focusing on performance outcomes. If combined with other tools, including baseline assessments, advanced technologies, training and exercises etc., they can help improve behavior and thinking. Standards are not the solution; they are one of the tools for cyber defense.

Recommendations and Conclusions

Cyber security incidents are increasing in both scope and scale every day. Our defensive mechanisms have been outpaced by the scope and scale of malicious cyber activities and, as a result, this issue now sits as one of the most important emerging security challenges facing our countries today. The North Atlantic Treaty Organization (NATO) recognized that it must improve capacity for Computer Network Defense (CND) and call attention to effective practices for incident detection and response. The Advanced Research Workshop, entitled 'Best Practices in Computer Network Defense (CND): Incident Detection and Response,' addressed this emerging security challenge. It brought together a multi-disciplinary team of experts from sixteen countries and three international institutions. Participants were selected from industry, academia, and public institutions who have direct hands-on experience with and responsibilities for incident detection and response. This chapter captured the rich discussion and debate from the workshop and highlighted the contributions of participants' technical presentations. In summary, twenty-one specific findings outlined how NATO member state and partners can improve their respective and collective cyber defense postures. These findings were:

1) Detection has replaced defense as a strategy.

2) Advanced, effective techniques for defense are operating in industry and showing promising results.

3) National strategies are rarely written as risk and threat based; they outline organizational roles and missions.

4) Threat assessments increase understanding and document trends.

5) Closing the gap between policy maker understanding and front line realities is essential.

6) Awareness is not enough; it should lead to informed action.

7) Member states are establishing unique learning and response mechanisms.

8) Political commitments may be equally effective (binding) as legal agreements and treaties.

9) Member states are investing in disruptive innovation and considering disruptive regulation.

10) Regulated and directed coordination rarely leads to trusted information sharing.

11) Effective (best) practices exist but are underused at organizational, sector, national, and international levels.

12) Formal and informal relationships and networks are equally important.

13) Identifying critical services is more important than identifying critical infrastructures.

14) A baseline assessment is essential to measure current and future effectiveness.

15) Training and exercising for crisis management situations builds relationships, processes, and confidence.

16) Qualitative and quantitative metrics inform decisions, test hypotheses, and forecast future states.

17) There is not enough research or discussion on recovery and reconstitution.

18) Military specifications can raise the bar on industry solutions.

19) Acquisition, purchasing, and security decisions are not mutually reinforcing.

20) Conflicting and competing standards exist now and need resolution.

21) Standards are only one way to improve security—not the way to improve security.

This chapter informs NATO cyber defense policy and presents operators and decision-makers with genuine tools and expert advice for computer network defense, incident detection, and incident response. The following chapters of this publication comprise expert research and technical insights that will continue to advance CND and directly support NATO's strategic goal to improve the level of cyber defense within the geographic scope of the Alliance and its partner countries.

References

[1] For example, notification is required no later than 24 hours after having become aware of the data breach in the European draft Directive on Network and Information Security.

[2] European Network of Transmission System Operators for Electricity (ENTSO-E), 2013. Network Code on Operational Security. [online] Available at: <https://www.entsoe.eu/fileadmin/user_upload/_library/resources/OS_NC/130227-AS-NC_OS_final_.pdf> [Accessed 15 November 2013].
[3] SANS Institute, 2012. Twenty Critical Security Controls for Effective Cyber Defense, version 4.1. [online] Available at: <http://www.sans.org/critical-security-controls> [Accessed 29 October 2013].
[4] Hathaway, M. E., 2010. Beyond Availability: Melissa Hathaway on the Cloud. Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at: <http://belfercenter.hks.harvard.edu/publication/20250/beyond_availability.html?breadcrumb=%2Fexperts%2F2132%2Fmelissa_hathaway%3Fpage%3D2> [Accessed 18 November 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-19

Computer Network Defense: New Threats and Trends

ANDREA RIGONI[a] and GUSTAV LINDSTROM[b]
[a]*Global Cyber Security Center (GCSEC)*
[b]*Geneva Centre for Security Policy (GCSP)*

Abstract. New technology trends invariably impact prospects for computer network defense (CND) – including the protection of critical infrastructures and services. Three evolving trends that stand out in particular include: 1) critical infrastructures' increasing reliance on commercial off the shelf (CoTS) technologies; 2) societies' growing reliance on mobile technologies coupled with a movement towards the 'Internet of Things;' and 3) the advent of cloud computing and big data. While these ICT trends contribute to economic growth and development, they will also generate new vulnerabilities, many of which may negatively impact segments of society. While policymakers play an important role in strengthening cyber security and resiliency, they may not always fully grasp the security implications of these and other technology trends – including the potential for ripple effects across different critical services and sectors. Minimizing this knowledge gap, as well as bringing tighter alignment and shared understanding of the operational realities and policy implications associated with new trends, is essential to promote effective computer network defense.

Keywords. Big data, cloud computing, computer network defense, control systems, critical infrastructure, cyber security, decision-making, information communications technology, Internet of Things.

Introduction

Given the increasing reliance on information communications technology (ICT), it comes as no surprise that the number and type of ICT attacks has also grown exponentially since the early 1990s. More troubling, ICT threats today are becoming more sophisticated and, in many instances, easier to develop or execute. Individuals and organizations that want to purchase ready-made malicious software can do so from a variety of on-line resources. Those with bigger budgets may opt for software security holes. For example, the purchase price for an Adobe reader vulnerability is in the range of $5,000-$30,000.[1] According to the most recent Symantec 'Internet Security Threat Report,' targeted attacks rose by 42% in 2012.[2] This increasing number has been driven by many factors, and in particular by an increasingly sophisticated black market serving a multi-billion dollar online criminal industry.[3]

Equally worrisome, but less well known, is that critical infrastructures (CIs) can be targeted via electronic means. Since they are increasingly dependent on information technology to operate and provide their services, the possibility of denying their activities is no longer an unrealistic scenario. At the same time, globalization is pushing critical infrastructure operators to merge and become large international groups, with

operations in multiple locations running dispersed and complex information systems, further reinforcing present vulnerabilities.

This chapter examines computer network defense (CND) and highlights the challenges faced by critical infrastructures. It focuses on three technology trends and the potential opportunities and threats associated with each. The chapter concludes with key areas that policymakers should monitor in order to plan and prepare for the future.

1. New Trends and Threats

ICT has been at the forefront of technological change for the last fifty years. Computing platforms (including computers, mobile devices, and next-generation capabilities) are now pervasive throughout our critical infrastructures, businesses, and society. As ICTs mature, they spawn new applications, contributing to economic opportunities through innovation. They also open the door to new types of risks and threats.

It is important to note that technological trends do not lead directly to new threats. In most cases, new technologies and systems also bring new security countermeasures and techniques but in some cases, new technologies may trigger new threats and vulnerabilities. Table 1 identifies some of the principal technological trends that might expose information systems to new vulnerabilities and threats. Needless to say, some trends are not included in the table, for example the evolution of cyber crime, which impacts our ability to achieve computer network defense.

Table 1: Computer Network Defense and Critical Infrastructures: Select Trends and Threats

Trends	Potential Threats
Critical infrastructures' increasing reliance on commercial off the shelf (CoTS) technologies in times of greater societal dependence on their services	- General lack of awareness of potential risks - Vulnerable industrial control systems - Attempts to circumvent basic authentication mechanisms - Possibility of cascading effects across CIs
A growing reliance on mobile technologies and the 'Internet of Things'	- Systems with no security features in their design - Weaknesses arising from improperly protected / patched devices - Greater complexity – leading to operational architectural and organizational complexity-outpacing human ability to comprehend how all pieces work together - Unintended consequences such as greater difficulty in achieving computer network defense
Advent of Cloud Computing and Big Data	- Risks to integrity and availability of data; - Potential for improper use of data; effects on privacy

The following paragraphs will focus on the three trends identified in Table 1 and the associated threats. These include:

- Critical infrastructures' increasing reliance on commercial off the shelf (CoTS) technologies;
- The growing use of (unsecure) mobile technologies and reliance on the Internet of things; and
- The advent of cloud computing and compilation of big data.

1.1. Trend 1: Critical Infrastructures' Increasing Reliance on Commercial off the Shelf (CoTS) Technologies

From the outset, critical infrastructure operators developed and acquired industrial control systems (ICS) to automate and digitize tasks traditionally carried out by humans. ICS are computer-based systems that monitor and control sensitive processes and physical functions. For example, they may collect sensor data from the field, forward information to appropriate destination points, and facilitate the relay of commands to local or remote assets. Such tasks may include monitoring temperatures, ensuring flows rates in pipes, setting thresholds for preventive shutdowns, and opening or closing circuit breakers. ICS systems are particularly important for the proper functioning of the energy, telecommunications, and transportation sectors. They usually fall into one of two categories:

- Distributed control systems (DCS): Used to control large and complex processes – usually within a single plant. DCS can be found in power plants, refineries, and chemical plants to assist with processing operations. Several types of controllers are used within DCS, including programmable logic controllers, machine controllers, process controllers, and single loop controllers.
- Supervisory control and data acquisition (SCADA): Used to control dispersed assets. They are generally employed in water systems, electrical lines, and gas pipelines to facilitate distribution operations. SCADAs may span several facilities, relying on remote terminal units and programmable logic controllers.

These two systems are not mutually exclusive; a critical infrastructure may use both types of ICS. For example, an electrical power infrastructure may use a DSC in its power generation facilities, while employing SCADA systems in the electricity distribution process. A similar pattern is discernible in the oil and gas sector, where DCS are employed in the refining and processing phase, while SCADAs assist with the distribution process.

Industrial control systems are often considered to be the intersection between the physical and cyber worlds. Given their ability to impact physical processes, a compromised ICS can in theory impact the health and safety of individuals, cause damage to the environment, negatively impact the economy, or compromise proprietary information.[4] As a result, there is a growing emphasis by governments and organizations on ensuring their proper functioning. Unfortunately, this is becoming more difficult as companies increasingly rely on commercial, off the shelf technologies (CoTs) to interphase with ICS.

As discussed in *Meeting the Cyber Security Challenge*, 'ICS were initially designed with proprietary technology and were separate from other existing corporate networks, such as local area networks and wide area networks.'[5] Networks connecting sensors and actuators were isolated, often relying on electrical and analogical connections. 'Because of this separate architecture, the systems were not prone to external electronic attacks.' Over time, however, the nature of ICS changed. Today, control systems are designed with networking capabilities embedded, and many older networks are connected to control networks through specific interfaces. The drive for cost efficiency and availability of commercial off the shelf (CoTS) software and hardware led to a gradual incorporation of new systems. By interlinking old corporate networks with new ICS technology, management is now able to receive real time data directly from the control systems, facilitating corporate decisions and improving performance. As a result, many of today's ICS are increasingly connected to the Internet.

From a security standpoint, connecting industrial control systems to the Internet has important implications. First, 'it exposes the control systems to hacking attempts, malicious software, and a number of other vulnerabilities that can be introduced through the Internet, intranets, remote dial-up, and wireless applications. […] The vulnerability is compounded by the merging of common information technologies such as Ethernets, Windows, and Web Services into ICS.'[6] A survey of 700 SCADA operators illustrates this growing security concern, with roughly 70% of respondents assessing the risks to their systems as high to severe and 33% suspecting they may have already had incidents.[7]

Second, connecting ICS to the Internet limits efforts to ensure adequate safety, given the overarching focus on efficiency. Many ICS run on older processors – such as Intel 8088 and 286s – and do not support new security updates such as encryption. As a result commands, usernames, and passwords are frequently passed in clear text over the Internet. Individuals and groups can easily intercept this information through packet sniffing tools. Exacerbating this vulnerability are systems that do not have the bandwidth, memory, and processing power required to incorporate existing security technologies such as authentication, intrusion detection, and filtering of network traffic and communications.

Third, the electronic vulnerability of critical infrastructure is magnified by the multitude of entry points available. In addition to direct access gained through stolen commands, user names, and passwords, attackers can enter via numerous access points that rely on limited authentication procedures. A number of critical infrastructures use dial-up applications, wireless access, Internet Service Provider (ISP) networks, and virtual private networks to facilitate access to grids, systems, and assets. These options are increasingly popular since they speed the process of diagnostic and repair operations. Using these systems, an operator checks to see if there are any repairs needed on a remote system. To facilitate access on a 24/7 basis, the systems tend to rely on limited authentication procedures – for example the use of a single username and password for external operators.

As reliance on CoTs systems that do not have adequate security features embedded continues to grow, it is likely that the number of attacks on ICS will rise, especially if there is a lack of awareness about such risks and organizations increase their reliance on open protocols and technologies. In 2010, there were 39 incidents reported to ICS-CERT.[8] In the first half of fiscal year 2013 alone, ICS-CERT responded to over 200 critical infrastructure breaches. According to them, the most common attack techniques

involved watering hole attacks (hijacking websites and then waiting for potential victims to connect in order to infect them), SQL injection (in which SQL commands are injected using vulnerabilities of the interface to attack an application and its data), and spear-phishing attacks (a customized form of phishing in which a criminal seeks unauthorized access to confidential data. This type of attack targets specific organizations or individuals).[9] Two well known-examples of intrusions into industrial control systems are:

- A cyber intrusion in 2011 at the Curran-Gardner Public Water District (Illinois) caused a water pump failure.[10]
- In 2000, a former employer of Maroochy Water Services in Australia compromised a SCADA system in the waste treatment facility, resulting in 800,000 liters of raw sewage being spilled into local parks, rivers, and the grounds of a Hyatt Regency hotel.[11]

The highest percentage of incidents reported to ICS-CERT in the first half of FY 2013 occurred in the energy sector (roughly 53%), followed by the critical manufacturing sector (17%).[12] With a steady growth in the global oil and gas sector, estimated to reach a market value of $4 trillion by 2018, it is likely that energy-related critical infrastructures will continue to suffer the majority of attacks in coming years.[13]

In spite of these challenges, there is some good news in this area. Most advanced countries now have national regulation and national plans in order to identify critical services and define protection plans for critical infrastructure operators. With respect to the identification of critical services, although they may vary from country to country, most include electricity production, transportation and distribution, water management, transportation, financial services, and telecommunications. As for protection plans, several organizations in North America and Europe have started to develop protection guidelines. For example, one of the initial organizations to work in this area was the North America Electricity Reliability Corporation (NERC), a non-profit corporation based in Georgia, USA. In 2008, NERC published its first version of the Critical Infrastructure Protection standard (now at version 3, with version 5 under Federal approval).[14] Since the release of this initial document, NERC has worked not only to introduce new technical controls, but also to change the overall approach and governance in the energy sector.

1.2. Trend 2: A Growing Reliance on Mobile Technologies and the 'Internet of Things'

Computer network defense is often associated with restrictive measures, such as strong authentication procedures and limiting the rights of computer users on a network, essentially creating virtual machines to tap into corporate programs and files.

A parallel and counterbalancing trend is the growing reliance on mobile technologies, many with limited security features. 'Bring your own device' (BYOD) exemplifies this tendency as employers increasingly rely on a mixture of professional and personal IT-platforms to work from home or while traveling. Many employers have embraced BYOD policies, arguing that it lowers capital costs while promoting staff productivity, agility, and availability. According to the SANS 'Mobility/BYOD Security Survey,' 61% of respondents indicated that their organizations' mobility policy allows them to use personal devices such as smartphones, tablets, and laptops for work.[15] This trend is reinforced by an explosive growth in sales of smartphones

and the increasing availability of applications. In 2011, for example, the sale of smartphones outpaced the sale of PCs; 488 million smartphones were sold compared to 415 million PCs.[16]

The gravitation towards mobile devices complicates computer network defense in at least three different ways.

First, companies are realizing that the benefits of mobile technologies and BYOD, such as greater productivity, are tempered by greater risks, such as unwarranted access by third parties, loss of proprietary data, and increase in network attacks. These risks can be further magnified if users rely on unsecure mobile technologies or are unaware of the dangers of plugging mobile devices into corporate networks. Risks are also accentuated when BYOD policies are applied to laptops, where the user has a lot more control on the operational environment. Corporate IT departments are struggling to manage new IT user environments composed of a variety of platforms from different vendors. Some of the most relevant threats relate to:

- Access and authentication to devices—this is especially relevant when a device cannot be properly protected, essentially allowing unauthorized users to access it;
- Email—the use of personal device email systems to access multiple accounts can lead to data loss, malware contamination, and privacy breaches;
- Stored data—personal devices can store corporate data locally, which could be exposed to local vulnerabilities and lead to corporate data leakages; and
- Malware—personal devices are solely under the control of their owners, who can install any kind of software and application, including unintentional malware (Trojans, Viruses, Worms, etc.), which can compromise not only personal devices, but also corporate services and data.

To mitigate these risks, organizations seek to strike a balance between IT security and mobility needs. One way organizations do this is by allowing the use of personal mobile devices that meet certain standards – such as smartphones with IPv6 support – or the use of virtual private networks (VPN).[17] Even if some corporations are taking steps to mitigate BYOD risks, there are other areas that are not easy to address, such as the storage of emails and corporate data on personal devices.

Second, most industries do not have the right internal skills to address computer network challenges that could affect their products. Amplifying this risk is a tendency to add 'networking features' to traditional products, with limited or no understanding of security requirements. As a result, there have been multiple examples of attacks against products that were not conceived with security in mind—a recent example is the intrusion into the USAF Predator drone.[18] This and other incidents led the US Federal Communication Commission (FCC) to consider new requirements for commercial products intended to connect to networks.

Third, the mobility/BYOD trend has led to a rapid growth in the number of devices connected to the Internet. Known as the 'Internet of Things,' this phenomenon ranges from devices equipped with networked sensors and actuators, which enable them to monitor their environment, receive instructions, and take actions, to the latest generation of smart phones.[19] According to one estimate, today there are over nine billion devices connected to the Internet across the globe, compared to 200 million in 2000. This figure is expected to grow substantially in coming years, with estimates

ranging from 50 billion to 1 trillion connected devices within the next ten years at which point the trend will be referred to as the 'Internet of Everything'.[20]

The number of devices that can be connected to the Internet is increasing daily, including every-day items such as home appliances, light bulbs, electric switches, thermostats, audio systems, cars, alarm systems, personal care devices, medical devices (e.g. insulin pumps), wearable devices, and weather stations. Through the use of technologies such as Radio-frequency identification or Smart Tags, it will be possible to connect objects to the Internet that were not originally designed to do so, providing a virtual representation connected to their status, for example location and environmental conditions. This is leading to billions of new devises connecting to the Internet that will inevitably broaden the attack surface, introduce new vulnerabilities, and increase the dependency of critical services (logistics, transportation, manufacturing, etc.).

While there are many positive dimensions associated with the Internet of Things, such as the potential to create an economic impact of $2.7 trillion to $6.2 trillion annually by 2025, there are also many concerns over the millions of vulnerable assets added and enhanced risks for cascading effects, where an attack on one sector could spill over to another.[21] The risks are compounded by potential new interactions between devices. As new protocols are developed to facilitate new levels of interactions between devices, this could also lead to unpredictable data flows and unexpected interdependencies (e.g. in the area of Machine to Machine Communications). In essence, the attack surface will become much broader, exposing new vulnerabilities, mainly due to the lack of vendors' experience in this area and the use of new protocols and functions that have not been tested properly.

As the Internet of Things evolves, there will be millions of connected devices that were not designed or implemented with built-in security, and that rely only on 'bolt-on' patches. All these systems are likely to become more complex over time, while retaining some degree of vulnerability that could compromise other platforms. For example, a passenger display in the aisle of a train that relies on an embedded version of Windows could be exploited. Modern trains are being equipped with many networks, some of which are open to passengers (on board Wi-Fi networks). This creates the possibility of leveraging a zero-day or unpatched Windows vulnerability on the display to gain access to the more critical control networks. While protections should be in place, the sheer complexity of such a network could result in exploitable vulnerabilities.

1.3. Trend 3: Advent of Cloud Computing and Big Data

Cloud computing is not new. It is a service architecture enabled by other technological trends, such as network/Internet bandwidth availability and virtualization. Nevertheless, the rapid adoption of cloud computing services in many sectors is exposing organizations and users to new risks. By 2014, IT organizations in 30% of Global 1000 companies worldwide will broker (aggregate, integrate, and customize) two or more cloud services for internal and external users, an increase of 5% from 2013.[22] It is estimated that the value of this market will grow from $46 billion in 2008 to more than $150 billion by 2014. The cloud is very appealing to both end users and corporations. While consumers use the cloud mainly for services such as email, music, file sharing, backup, and personal productivity, corporations can choose from a variety of services, including infrastructure as a service to enable sales force automation and enterprise resource planning.

One of the biggest risks posed by cloud computing is the consolidation of systems and data in large infrastructures managed by a single operator. Many customers, sometimes in the order of hundreds of thousands, share the same facilities, infrastructures, and systems. While these giant infrastructures are generally well protected – they typically provide a higher level of security than single customer organizations – there are nevertheless risks that, in the event of a breach, a large number of customers could be affected. This threat is particularly relevant for cloud services delivered through large shared infrastructures, such as data centers, storage, servers, applications, and middleware. A related risk factor is the externalization of control: organizations are used to manage security internally, often focusing their attention on technological countermeasures. Cloud services force organizations to adopt new tools to control security, shifting their attention from countermeasures to control and legal agreements. This risk could easily become an opportunity, as it forces organizations to approach security from a risk management perspective.

Beyond the challenges discussed above, the cloud presents additional issues that ought to be considered. For example, the Cloud Security Alliance's (CSA) report on 'The Notorious Nine: Cloud Computing Top Threats in 2013' identified nine of these critical issues, which are briefly summarized below.[23]

1) Data breaches: these represent one of the more serious cloud computing threats because of the possible theft of corporate confidential data. In November 2012, a research study from the University of North Carolina demonstrated that it was possible to extract cryptographic keys from a machine by using another virtual machine.

2) Data loss: data stored on the cloud could be lost for many reasons, including attacks, intrusions, faults, and poor maintenance.

3) Account hijacking: malicious actors could take control of a cloud service by hijacking accounts. This could result from bad cloud service configurations (as with cross-side scripting vulnerabilities), from external attacks on users via phishing, or the use of malicious software on the end user side, in particular when simple authentication systems are in place.

4) Insecure Application Programming Interface (API): cloud services interact with users through interfaces or API that in some cases could expose the service if not secured properly.

5) Denial of Service: DOS attacks are still very common and have become ever more sophisticated in recent years. Cloud providers are an ideal target for DOS attacks and, in the case of shared infrastructures, attacks as asymmetric application-level DOS could affect a large number of customers.

6) Malicious insider: internal employees, contractors, and administrators with access to organizations' infrastructure, services, and sometime customer data could intentionally misuse or compromise cloud services.

7) Abuse of cloud services: cloud services could be used to perpetrate malicious activity, such as DOS attacks, encryption key cracking, distribution of malicious code, etc.

8) Insufficient due diligence: when applications and services are moved to the cloud, organizations delegate many operational aspects to the cloud service provider. Even if customers delegate the management of their security to a third party, they should not take its implementation for granted. Organizations should have capable resources, and perform extensive internal and CSP due-diligence to understand the risks they assume when adopting this new service model.

9) Shared technology issue: this is one of the key risk factors, as the use of shared infrastructures could expose not only the compromised customer, but all customers served by the infrastructure.

In addition to the nine critical threats identified by the Cloud Security Alliance, there is a tenth threat area related to international law and law enforcement. It concerns dispersed infrastructure and data storage. Since cloud computing data can be stored and processed in other countries, data delocalization could have legal and law enforcement implications.[24] With respect to legal aspects, data could be subject to diverging national laws, such as data protection and data breach notification requirements. As for the law enforcement issue, data that may be legally stored in the customer's home country may not be legal in the country where the cloud computing service actually stores that data.

According to one estimate, the cloud computing market will grow at a 36% compound annual growth rate (CAGR) until 2016 and affect all sectors.[25] In addition, cloud-computing solutions are being developed for critical services such as smart grids, exposing these sectors to new risks. While this trend provides an economic opportunity for operators, reducing operational costs and increasing service quality and reliability, it also exposes operators and cloud computing companies to new threats that they may not be ready to manage yet. Moving to the cloud should be a thoughtful process. Operators should start by improving their security governance frameworks and negotiating with cloud computing companies to ensure that the right security controls are aligned with corporate cyber security policy.

Recommendations and Conclusions

While current ICT trends contribute to economic growth and development, they also create new vulnerabilities, many of which can negatively impact substantial segments of society. The combination between continuous ICT developments and policymakers' general lack of awareness about cyber risks further complicates the ability to achieve a robust computer network defense.

Some the principal trends that policymakers should monitor are:

- The effects of an increasing use of CoTS technology to provide critical services;

- The ramifications of greater reliance on mobile technologies coupled with the evolution of the Internet of things; and
- Developments in cloud computing.

A host of challenges may materialize within each of these categories – including the risk of cascading effects across different critical services or sectors.

Policymakers should also be aware that there are strong interlinkages across these trends. For example, the movement towards the Internet of Things is likely to affect a variety of sectors, connecting security within critical infrastructures to the way society interacts and organizes itself. As more platforms are connected to the Internet, the attack surface will also inevitably broaden, something that groups and countries with malicious intent will try to leverage. Policymakers will also need to consider how greater interconnectivity, system complexity, and access to large data might lead to additional vulnerabilities with high potential for spillover, and affect non-tangible rights such as the right to privacy. In brief, there will be a premium on the ability to respond to both the intended and unintended consequences of ICT developments across society.

References

[1] Greenberg, A., 2012. Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. Forbes Magazine, [online] Available at: <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/> [Accessed 6 November 2013].

[2] Symantec, 2013. Internet Security Threat Report 2013 [pdf] Symantec, p. 20. Available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf> [Accessed 6 November 2013].

[3] Ibid, p. 24.

[4] Stouffer, K., Falco, J., and Scarfone, K., 2013. Guide to Industrial Control Systems (ICS) Security. Washington, DC: National Institute of Standards and Technology, US Department of Commerce. [online] Available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf> [Accessed 6 November 2013].

[5] Lindstrom, G., 2012. Meeting the Cyber Security Challenge. Geneva Centre for Security Policy (GCSP). [online] Available at: <http://www.gcsp.ch/content/download/9408/113285/download> [Accessed 6 November 2013].

[6] Ibid. Meeting the Cyber Security Challenge.

[7] Luallen, M., 2013. SANS SCADA and Process Control Security Survey [pdf] SANS Whitepaper. Available at: <http://www.sans.org/reading-room/analysts-program/sans-survey-scada-2013> [Accessed 6 November 2013].

[8] US Department of Homeland Security, 2012. ICS-CERT Year in Review. Washington, DC: Industrial Control Systems Cyber Emergency Response Team, p. 12. Available at: <http://www.uscg.mil/hq/cg5/cg544/docs/Year_in_Review_FY2012_Final.pdf> [Accessed 6 November 2013].

[9] For a more detailed discussion on ICS vulnerabilities and threats, including recommendations for their mitigation, see Stouffer, K., Falco, J. and Scarfone, K., Guide to Industrial Control Systems (ICS) Security.

[10] Krebs, B., 2011. Cyber Intrusion Blamed for Hardware Failure at Water Utility. Krebs on Security blog, [blog] 18 November. Available at: <http://krebsonsecurity.com/2011/11/cyber-strike-on-city-water-system/> [Accessed 6 November 2013].

[11] Abrams, M., and Weiss, J., 2008. Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia [pdf] The MITRE Corporation. Available at: <http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf/> [Accessed 6 November 2013].

[12] ICS-CERT Monitor, 2013. Incident Response Activity: Brute Force Attacks on Internet-Facing Control Systems [pdf] US Department of Homeland Security. Available at: <http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf> [Accessed 6 November 2013].
[13] The Wall Street Journal, 2013. Research and Markets: The Global Oil and Gas Market Value Will Continue Growing At an Improved CAGR of Nearly 4% Right Through 2018, Reaching About US$ 4 Trillion of Market Value By 2018 (Press release), Business Wire, 12 March. Available at: <http://online.wsj.com/article/PR-CO-20130312-913993.html?mod=crnews> [Accessed 6 November 2013].
[14] North American Electric Reliability Corporation (NERC). Critical Infrastructure Protection Standard v. 3. Available at: <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx> [Accessed 6 November 2013].
NERC. Critical Infrastructure Protection Standard v. 5. Available at: <http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20Comments%20to%20CIPV5%20NOPR%20_%20FINAL.pdf> [Accessed 6 November 2013].
[15] Johnson, K., 2012. SANS Mobility/BYOD Security Survey. [pdf] SANS Whitepaper. Available at: <https://www.sans.org/reading-room/analysts-program/mobility-sec-survey> [Accessed 6 November 2013].
[16] Mewada, A., 2012. Smartphone Overtook PCs for First Time. Digit Spark, [online] Available at: <http://www.digitspark.com/2012/02/smartphones-overtook-pcs-for-first-time.html> [Accessed 17 November 2013].
[17] For additional information on ways to minimize BOYD risks, see: CDWG, 2013. Securing BOYD: Guidance on the strategies and tools needed for a secure and productive bring-your-own-device program. [online] Available at: <http://www.edtechmagazine.com/higher/sites/edtechmagazine.com.higher/files/byod-security-g.pdf> [Accessed 6 November 2013].
[18] Rashid, F. Y., 2011. U.S. Strategic Drone Fleet Infected by Stealthy Keylogger Malware. eWeek, [online] Available at: <http://www.eweek.com/c/a/Security/US-Strategic-Drone-Fleet-Infected-by-Stealthy-Keylogger-Malware-561651/#sthash.SHEfuPmo.dpuf> [Accessed 6 November 2013].
[19] Manyika, J., et al., 2013. Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute.
[20] Bradley, J., Barbier, J., and Handler, D., 2013. Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience. [pdf] CISCO Whitepaper. Available at: <http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf> [Accessed 6 November 2013].
[21] Manyika, J., et al., 2013. Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute.
[22] Columbus, L., 2013. Roundup of Cloud Computing & Enterprise Software Market Estimates and Forecast, 2013. A Passion for Research [blog]. Available at: <http://softwarestrategiesblog.com/tag/idc-saas-forecasts/> [Accessed 17 November 2013].
[23] Cloud Security Alliance, 2013. The Notorious Nine: Cloud Computing Top Threats in 2013. [pdf] Available at: <https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf> [Accessed 6 November 2013].
[24] Hathaway, M., 2010. Beyond Availability: Melissa Hathaway on the Cloud. Harvard University Belfer Center for Science and International Affairs. [online] Available at: <http://belfercenter.hks.harvard.edu/publication/20250/beyond_availability.html?breadcrumb=%2Fexperts%2F2132%2Fmelissa_hathaway%3Fpage%3D2> [Accessed 6 November 2013].
[25] TheInfoPro, 2013. Cloud Computing Poised for Explosive Growth. New York: 451 Research [pdf] Available at: <https://451research.com/images/stories/Marketing/press_releases/cloud_wave_5_press_release_final.pdf> [Accessed 6 November 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-30

Advanced Technologies/Tactics Techniques, Procedures: Closing the Attack Window, and Thresholds for Reporting and Containment

JOHN N. STEWART
Cisco Systems and
Council of Experts, Global Cyber Security Center (GCSEC)

Abstract. New techniques, tactics, and procedures (TTPs) are now available to strengthen security postures and become more resilient to cyber threats. Most of these technologies are accessible and affordable, and they are showing promising results. This paper exemplifies eight specific advanced techniques, tactics, and procedures to counter cyber threats, including using moving target architectures to confuse the adversary, monitoring the dark space of the Internet, and using honey pots to detect adversaries and infected machines within an organization's infrastructure. It also explains what is required to enable these techniques and what metrics should be used to measure their results. These advanced practices should become common security standards.

Keywords. Advanced persistent threat, cyber attack, cyber security, dark space, data exfiltration, domain name service, honey things, honey tokens, identity, indicators of compromise, metrics, misinformation, moving target, patching, reconnaissance.

Introduction

Internet-connected devices have proliferated to such an extent that in 2008 more connected devices existed on Earth than people. The trajectory continues; some reports projecting that by 2020 the number of devices connected to the Internet will exceed 50 billion.[1] Cars are coming online, homes are automated with Internet Protocol (IP) based technology, hospital operating rooms have wireless networks, saltwater treatment plants are configuring IP addresses on the boilers for remote control and system feedback, and military systems are using connectivity and information as the warfighter edge.

The rapid spread of Internet-connected devices carries its attendant risk: a new piece of malware is detected every 2.2 seconds.[2] The number of breaches in the past twelve months exceeded 850, with 174 million records compromised.[3] A well-known DDoS campaign against various US banks has been ongoing for over a year. In two other examples, one company had 30,000 computers infected[4] and rendered inoperable via a directed attack, and a few others had the Advanced Persistent Threat 1 (APT1) hacking team active in their network for over four years, and all the while over 85% of breaches took at least one week to detect.[5]

The effects of such attacks are immediate and tangible: intellectual property (IP) and personal information stolen; services disrupted; systems erased; and networks compromised. Sophisticated hacking teams are very active and can operate entirely undetected for long periods of time.

It is equally instructive to note how dependent we are on technology for our day-to-day lives, including civilian and military operations. The mobile phone is the primary means of communication. Information availability is now the sought-after military and business operational edge against adversaries and competitors respectively. Our economy is now tied to this technology evolution: countries' GDP growth is directly affected by high ICT, be it when 10% of the population is connected, the GDP goes up 1-2%, or how digitization provided US$193 billion to the world economy in 2011.[6]

All told, we no longer use IT systems – we rely upon them.

The increase of connected devices and online services creates an expanded attack surface for would-be attackers. In other words, we now have a situation ripe for attacking combined with a robust population of adversaries who are increasingly motivated, trained, and confident. Given all this, we need to ask ourselves: 'What can be done now that tips the scales back in our favor, what does it take to get there, and how can I measure my progress?'

Included in this paper are eight advanced techniques, tactics, and procedures (TTPs) for meeting our needs head on, what is required to enable them, and five quantitative metrics to measure progress.

1. Advanced Tactics, Techniques, and Procedures

The security domain is an ever-evolving discipline where measure and countermeasure are developed in turn, and where new ideas emerge in all organizational verticals. New, emerging techniques are always coming to the fore. Twenty Chief Information Security Officers (CISOs) and security operators,[7] whose work protects companies worth over US$500 million in combined market cap, were interviewed for this paper. Their experiences and cutting-edge practice highlight three areas that reduce attack surface, lower the adversarial opportunity, and tip the scales in the defense's favor. These three areas are:

- Basics must be mastered:
  - Patching
  - Identity: Strong Identity, Federated Identity, and Identity Based Networking
  - Eliminate Dark Space
- Create doubt in the adversaries mind:
  - Moving Target
  - HoneyThings / HoneyTokens
  - Misinformation
- Analyze data and traffic for Indicators of Compromise (IOCs):
  - Local Data *Analytics*
  - Global Grids: The Eye in the Sky
  - Analysis of non-conformant protocol traffic, local or global

2. Basics Must be Mastered

We often believe that the latest technology will solve our problems, losing sight of what we can actually control—our own infrastructure. Do not be fooled by the seeming simplicity, because mastering the basics is actually an advanced approach. While the security industry continues to innovate, seeking another appliance, another software module, and another 'best practice', the fundamentals tend to remain the same. No matter how many modules and best practices exists, there are three elements to a successful attack: means, motive, and opportunity. Since an adversary's means and motive are generally beyond our control, we must focus on the one thing that is always within our control: opportunity.

2.1. Patching

Enterprise data rarely exists on certain metrics (patched systems, security architecture, vulnerabilities), but consumer data does. This is instructive for even the most hardened critics who argue that the two do not compare naturally. The average online citizen in Germany, for example, has 75 programs from 25 different vendors. Of these, 14% are using operating systems that are not fully patched, and another 7+% of the applications installed are also not fully patched.[8]

Even if, by comparison standards, we reduce this down to 1% for enterprises, there can be no doubt that the risk surface remains significant. That said, the risk exposure is higher, with 10% of enterprise company respondents indicating they have done a full job of implementing the basics, represented here as the SANS 'Twenty Critical Security Controls for Effective Cyber Defense.'[9] Implemented correctly, basics such as patching can begin to move the needle on the 'opportunity' scale, systematically reducing the attack surface which adversaries may breach.

Using formal methods, patches have an ability to reduce attack surface up to 67-70% just by application.[10] Patching has shown statistical evidence proving to reduce the attack surface, and yet the statistics also suggest that use of this effective method is inconsistent at best.

Note that patching is not just about servers and applications; it is also about the network – the fabric used to connect everything else. Using interview responses and experiential data, one can conclude that network maintenance, patching, auditing, and controls validation are areas lacking investment. Interestingly, with the network being the transport means for all other systems that connect, it would seem that this attack surface should be minimized due to its criticality.

2.2. Identity: Strong Identity, Federated Identity, and Identity Based Networking

A less obvious basic that must be mastered is identity. There are three parts to this: strong identity, federated identity, and identity based networking.

Statistically, most users do not use or are not required to use a strong digital identity and password. Two-factor and one-time password authentication should be universally deployed on critical systems, if only to avoid the simplest of exploits: co-opting the actual password from a user or administrator to gain unauthorized access to systems. The probability of such a breach can be reduced significantly with two-factor and one-time password authentication. The end result of such authentication procedures

is that core infrastructure takes more time and effort to successfully penetrate, a clear goal for all of us.

In addition, federated identity—in which a user's credentials can be used again without creating another account—makes for a user-friendly experience, reduces the total number of accounts, and simplifies forensics after an incident. This is not Single-Sign-On (SSO) exclusively, however, as the identity federation can often be between multiple identity brokers. The end goal here is to simplify the user experience while simultaneously increasing overall difficult for an adversary.

The last piece is a more advanced use for identity—identity based networking. In this area, a user's identity, coupled with a variety of factors such as the system they are using, time of day, and location, all play a role in what the user can do at any given moment. An example would be how a financial controller in a public company, upon login, will be able to see applications and services based on which system they are using (smartphone versus in-office computer), where they are currently located (the office or on the road), and what time of day they are aiming to use the service (3am versus 10am).

2.3. Eliminating Dark Space

In addition to standard methods such as traffic analysis, non-protocol traffic, and HoneyThings/HoneyTokens, one must also find and eliminate dark space, e.g. the 'blind spots.' Dark space is loosely defined in the security world and often refers to looking at the 'inverse' of what you see, to infer what you might need to know about it.[11] A simple example is a network map, where you see all the devices in your network, yet what you really need to know is if there are network interfaces that are 'up' and you do not see the other side of the connection, or that you are running network devices that seemingly have no connectivity to the core network.

Dark space can hurt in the datacenter world too, because if scanners cannot analyze blocked data center segments then the risk analysis is incomplete for the data center. Finding and eliminating dark space, however, can be difficult because we are frequently taught to look at what *is* there, and rarely are we asked to look at what *is not* there and ask questions about it. That is precisely the line of questioning necessary to tackle this issue. The dark space will contain risks so becomes a natural attack surface for the patient, skilled, and/or lucky adversary.

2.4. Summary: Basics Must Be Mastered;

Control what you can control, and do it well.

While things like patching, strong identity, or knowing your own infrastructure may seem obvious solutions rather than advanced techniques, leading practitioners are returning to the basics lower their risk through attack surface reduction. The reality is that while these solutions may sound like common sense, the activities mentioned—not investing in the latest malware detection versus fully investing in asset inventory and layer zero through seven services mapping,[12] deploying strong identity instead of fixed and complex passwords, and modeling and mapping the services your data center is providing—is actually quite rare. The 'basic' solutions turn out to reflect the most advanced thinking on the issue.

3. Create Doubt in the Adversaries' Mind

3.1. Moving Target

One can make a rational argument that the reason data center systems are frequently and easily compromised is that they are relatively stationary. Data center systems do not 'change' much from one day to the next—the IP addresses, service, machine names, and configurations change infrequently—so an adversary may study them over time. Moving targets, on the other hand, create confusion for the adversary and create more difficult environments to maintain persistence in, and are now technologically possible. Two moving target examples are virtualization and Software Defined Networks (SDN).

Using virtualization and virtual machine clusters in data centers, you can reboot at will and/or randomly without interrupting service. This 'start from scratch' approach makes the virtual machine jettison malware if infected, as well as interrupting any covert, undiscovered activity from continuing onto the host. Lastly, virtual machines can reset the system baseline, which can potentially illuminate a re-infection attempt if instrumented to do so. A key element to success in virtualization is Intel Trusted eXecution Technology (TXT) or similar capability, which helps ensure the software and service validity. Additionally, control instantiation must reinstate from a clean slate as well (virtual firewall context, for example), which defines a baseline known-good, further allowing for compromise detection.

Software Defined Networks (SDNs) are a new approach that separates decision-making in the control and data planes. In the security realm, SDNs have rather unique applications. For example, you can now choose which traffic to send through your bandwidth/processing restricted security engines such as Data Loss Prevention (DLPs) systems, instead of sending all of your traffic through them. You can make this decision on-the-fly, adding an additional flexibility for you and additional confusion for your adversary.

In addition, you can dynamically segment your network, which makes the network appear as if it was reconfigured. Alternatively, during a successful attack, you can dynamically quarantine infrastructure and systems. You can also create a 'ghost network' to confuse the adversary, increasing their cost and risk.

3.2. HoneyThings/ HoneyTokens

Honeypots are commonly used in networks to attract interest from adversaries, after which people study the adversary's techniques, slow them down, or ultimately defeat the adversary by detection. While HoneyThings and HoneyTokens are not new—the terms were coined nearly a decade ago—they are emerging as a sophisticated counter intelligence technique when used pervasively. Ghost machines in an infrastructure that have no real value, but look attractive; source code modules that essentially do nothing, and can be found in other products if IP is illegally copied; fake database accounts that are only interesting for malicious queries;[13] fake email addresses on mailing lists which will inform the owner if the list is copied; the list goes on.

The key here is baiting, where the value of the asset is not necessarily the asset itself, but rather the attraction and detection that result from another's interest in the asset. The end goal is detection, not prevention, and it may well be you can detect other machines infected or controlled within your own infrastructure or that you can affirm your IP was illegitimately re-used in another commercial product.

3.3. Misinformation

While the tactic is controversial to some, misinformation offers another route to create adversarial confusion. Misinformation campaigns include a range of tools, including: monitoring the underground anonymously; introducing false information; allowing a hacker to continue to operate uninterrupted in order to learn their technique (making them believe they cannot be seen); and many others. The major risk of misinformation is that you end up confusing both the adversary and yourself. In order for this method to be effective, the misinformation must only disrupt the adversary, otherwise it is best to be prepared for unintended consequences. For example, if you falsely communicated that an attack was unsuccessful—doing so, of course, in an attempt to create doubt in the adversaries' mind—even though it clearly was, you may also find yourself violating other controls if the truth were to emerge.

3.4. Summary: Create Doubt in the Adversaries Mind;

Shake the Confidence of our Adversaries.

In *the Art of War*, Sun Tzu wrote 'The whole secret lies in confusing the enemy, so that he cannot fathom our real intent.' In this case, our enemies are those attempting to illegally copy, disrupt, or destroy our information and systems, and one way to deter and defeat them is to confuse them using virtualization, HoneyThings, and even misinformation campaigns which can all lead them down a bridge to nowhere. In short, these tactics force adversaries to spend time and energy on path that are ultimately wrong, wasteful, and dangerous.

4. Analyze Data and Traffic for Indicators of Compromise (IOCs)

Too few organizations use the most powerful source they have: data. There are two complimentary methods for using data to disrupt attacks: local and global data analytics. Successful protection for your organization requires both.

4.1. Local Data Analytics

Local data *collection* is a common practice, while local data *analytics* on that data is not common, except forensically. Analyzing protocol traffic to ensure it is allowed to go to and from authorized places is standard practice, while dropping malformed packets and alerting the SOC it happened is incredibly rare. There is opportunity to level up here.

For advanced local data analytics, two data sources emerge:

- Netflow/jflow/ IPFIX and Domain Name System (DNS) data;
- Netflow/jflow/cflow are record formats that indicate, among other things, the source and destination IP addresses and ports which two systems attempted and possibly succeeded in communicating upon. A rudimentary comparison to 'call records' in the phone world, network and security operations leverage this for seeing Advanced Persistent Threat (APT) malware callouts, for data

exfiltration successes and attempts, and deployed internally to a network, lateral movement for malware from machine to machine.

Domain name system (DNS) traffic capture and analysis provides insight into where computers are seeking to go, as a result of seeing what 'name' on the Internet is asked for, security and network operators can see if well known bad sites are asked about by systems (e.g. are users going to known malware sites), or if unusual DNS activity is requested to resolvers such as a reverse pointer record (PTR)[14] which goes nowhere.[15]

A key question that needs an answer is this: what is good, and what is bad? The answers vary from organization to organization, and in the end, will likely be stitched together with base lining actual traffic, and then loading up known bad IP addresses, domains, command and control (C&C) server IP addresses and black-hole routes, using the combined list to check the local data to see if there are IOCs.

4.2. Global Data Analytics, the Eye in the Sky

Complementary to local data analysis is the subscription and connectivity to global data and threat analytic platforms. Anti-virus vendors, SPAM filters, and reputation analysis engines are online with sensors numbering in the thousands to millions. These global grids give each participant access to otherwise inaccessible data. In doing so, these systems provide machine level and human readable analysis which is more complete than any one of us could amass individually.

This connectivity can be machine based with web filters, BGP black-hole routes, email SPAM filters, and anti-virus, or can be human readable tailored threat reports, which provide a view from the outside to your network about IOCs.

4.3. Analysis of Non-conformant Protocol Traffic, Local or Global

An unintended security technology side effect is that IOCs are often unseen due to the technology *doing what it was designed to do and not more*. In an ironic twist of fate, when traffic is dropped purposefully to protect against threat, that dropped traffic may well indicate a second problem needing solving solution: a compromised host.

For example, a web proxy can inspect port 80, 443, and other pre-defined web port traffic to ensure that malware-laden websites are not connected to, questionable content is filtered, and authorized sites are permitted. This same technology, however, will often silently drop traffic that does not appear to be web traffic – and it is in *that* traffic that an IOC hides. DNS servers do much the same, as do email gateways, yet in each and every case if the dropped traffic were analyzed for IOCs, you increase the chances for seeing infected systems.[16]

4.4. Summary: Analyze Data and Traffic for Indicators of Compromise:

Use data to drive decisions, not emotion.

With local data analytics, 'your' world becomes clearer – which systems talk to one another, which are studied and attacked, which are vulnerable, which are resilient, and which are connected. Global data analytics connect the dots, so an attack campaign targeted at banks becomes clearer, as does a protocol attack against a specific

technology, which benefits us all. Studying non-conformant traffic in each shows how our adversaries try to hide using openings we authorized, just not for them.

5. Change the Mental Model

When it comes to security, changing one's *actions* is just as important as changing one's *thoughts*. For example, when you read a phrase like 'mastering the basics,' your gut reaction may be that such a thing is obvious—of course the basics should be mastered. The subtlety is that mastering the basics is not advanced *technologically*, it is advanced *intellectually*. Why? Today's security practices often lead us down a path to the latest technological tool or gadget, not realizing that 'good hygiene' (i.e., mastering the basics), likely lowers risk more.

5.1. Assume Compromise

Unfortunately, the reality is that what was once surprising is now normal: networks and environments are penetrated regularly and many network teams are now assuming they have been successfully penetrated and use detection as the vehicle to discover it. This mental model is inherently conflicted – the defense is presumed to have failed. Assuming compromise is not giving up; protecting critical systems is essential no matter what. This mental shift is about enabling detection.

5.2. Outsourcing

Another trend is the outsourcing of security to another organization, which carries both risk and reward. For example, if talent is not available to hire or the work cannot be managed internally, then outsourcing may be the difficult, and ultimately correct, choice. A lack of talent at your company may mean having someone else protect you. This is an intellectual leap, because security is core to the success of many organizations and to place that in other's hands can be difficult and uncomfortable.

5.3. Defeat the Adversary vs. Try and Stop them from Getting in all the Time

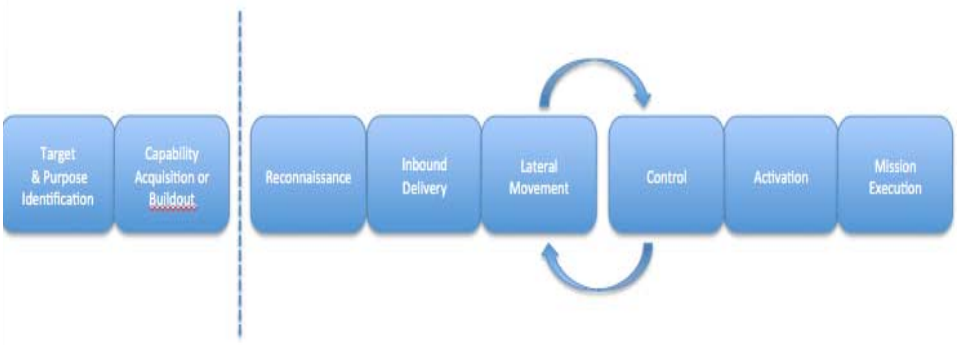


Figure 1. Cisco Systems Internal Kill Chain Model

A very subtle mental shift is to remember that stopping adversarial success is the most important goal, not necessarily stopping penetration or systems penetration per se. The

difficult thing to remember is that you can detect some things but not others, and that system infection does not equal operational failure *if the infection is not able to execute the mission*. This requires getting in the kill chain, to include detection of probes all the way to disruption in the final mission execution step.

5.4. Be Your Own Adversary – Hack Yourself

Aggressively attacking your own infrastructure requires an intellectual leap: to best prepare yourself for anything, practice war gaming with live ammunition (exploits) on live targets (production systems).

Auditing your own infrastructure is a known practice for protection, although it has limited value as generally practiced today. Hacking (not auditing) yourself with your own team, however, has emerged as an entirely different, and possibly quite controversial, approach. The rationale behind the new method is that the hackers do not behave like auditors; they do not have predictable timeframes for their work, they break rules and laws, and they spend significant time in some cases before launching their attacks against critical infrastructure. So, the question is: why not behave just like they do?

To make the impact of a security threat real, it must personally affect an IT professional, a business executive, or a key developer. Acting like a true adversary (cognizant that the service you are attacking may go down, be corrupted, require costly repairs, etc.) is the new approach – you are acting just like the hacking community, and in doing so, preparing thoroughly. An unanswered question is: is hacking your own systems the right thing today to make it real?

5.5. Whitelisting

It is ironic in the security world that we keep looking for the 'bad'—even though it is infinite—without focusing on known good, which is finite and achievable via whitelisting. Sometimes called the panacea for computer security, whitelisting is now practically applied as a noise reduction technique for both on-host, file whitelisting, for DNS domains for network flows, SPAM email gateways, and increasingly, for Cloud-based services. The underlying principle here is moving from 'blocking bad, and implicitly allowing everything else' to 'permitting good and denying everything else.' It can be said, unscientifically, that security's major practices are still in the first category.

Whitelisting takes multiple forms. On-host, it is all about legitimate files that do not need inspection since they remain whitelisted as good. For DNS, it is about dynamic domain filtering to determine good versus bad in a domain lookup. For traffic flows, it is topological knowledge about network configurations so that known traffic is permitted and all other traffic is implicitly denied.

The caution on these systems is remaining current, implying that knowing where to keep current on known good files, flows, domains is the essential component, and more often than not, not a core skill set for an organization to maintain themselves.

5.6. Summary: Change the Mental Model

What got us here today will not carry us forward into the future.

Too often, common practice becomes correct practice, and in so doing, the needed changes are difficult to absorb, since we have trained ourselves to believe in the common. Mental model switches are essential in our industry right now because our mental models are holding us captive.

6. Progress Indicators and Thresholds: Metrics

You get what you measure, as management training asserts, and this field is no different. Yesterday's metrics were binary: breached or not. Today's metrics are combinatorial: breached or not, and the breach's impact. Tomorrow's metrics, which arguably some leading member states and companies are using now, are catalysts: adversarial dwell time, adversary confusion ratio, compromise speed, cost to protect vs. cost to lose or restore, and mitigation coverage percentage.

6.1. Adversarial Dwell Time [17]

Measuring how long the adversary is inside your walls prior to you noticing is a lagging indicator that shows how effective your detection process is. Revisiting a common theme—opportunity—this particular metric helps gauge two things: how effective are you in seeing an adversary, and how long your adversary has to execute a mission. While the adversary may well be 'you' in this case (e.g. sponsored hack-a-thon activity), limiting time to detection and time for mission execution are the correct goals.

Dwell time can be safely detected by having red-team exercises, and these will both tell you how fast something is detected, and how fast the activity is disrupted. If not fast enough for both, the red-team mission may well succeed. Because you control both the attack and defense in these exercises, both will learn.

Forensics also provide insight into dwell time, namely research into a successful attack build, a timeline that sometimes goes all the way back to the reconnaissance.

6.2. Compromise Speed

Consistent with adversarial dwell time is compromise speed. In measuring how long it takes various sophistication levels to compromise, disrupt or destroy a target, you learn if the target's protection and resiliency are up to the level expected. To measure effectively means to act like the adversary, either you or a provider. Red Team/Blue Team exercises are often designed with this goal in mind. These exercises are not fully effective as they otherwise could be, however, due to legal restrictions imposed on one of the teams (restrictions which your adversary will ignore). To be truly ready to face your opponent, then, you must think and be able to act like him.

There are multiple adversarial models to be considered. These include, but are not limited to:

- Having internal organizational knowledge;
- If the adversary completed some or significant reconnaissance;
- Was there insider assistance for the attack;

- Malware capabilities (to include at what level, ability to deploy, targeted not targeted);
- Value for the target.

In the end, the goal is to properly model whether your valuable assets, information or services can remain resilient long enough before the 'dwell time' timer for your organization, on average, expires and detection and countermeasures disrupt the attack.

6.3. Unmitigated Attack Duration

It is accepted that attacks come in different forms, and if an attack is successful quickly, yet the effects are prolonged, then the attack itself is only halfway to measuring the overall duration. For example, if intellectual property is stolen via a compromised computer, the computer compromise is only one part of the attack's duration. Attack duration is the time from beginning to end of the kill chain (see Figure 1), and may not easily be measured, as you won't always know when *Target* and *Purpose Identification* happened.

That said, some attacks such as DDoS do have an ability to be measured for success from the beginning to the end, and the time in which the attack is effective becomes the metric to use. There are multiple ways to measure this mathematically, starting with the 'time the attack began until the time the mitigation abated the attack.' This may be augmented by using lost revenue or cost to mitigate (see below on mitigation vs attack costs), which aid in true cost through weighting. Why? Because the first five minutes of an attack may well be much more costly than the next fifteen minutes, even if the entire twenty minutes were before the mitigation. For example, if a financial trade must be completed by 1pm, the attack starts at 1255pm and lasts for twenty minutes, the first five minutes were the most costly – because the trade did not happen, and the mitigation didn't arrive fast enough.

6.4. Adversarial Confusion Ratio

One of the elements that affect Compromise Speed and Dwell Time is adversary confusion, e.g. the delays injected into the mission and its goals due to confusion in the adversary's mind.

The adversarial confusion ratio is calculated in two pieces. Take the time confused divided by the total time, and take the number of incorrect decisions created by countermeasures versus the total made. Unless able to talk to your adversaries, which as strange as it might seem does happen from time to time, you will need to rely on Red Team/Blue Team exercises to know for sure.

Technological implementations already proven today include rebooting virtual servers randomly, and over short periods, to eliminate persistent command and control; using software defined networks to dynamically re-route traffic into a simulated environment, thus removing the conflict from the production environment; and using IPv6 enumerated networks to create a broad threat surface to have to hunt in, while simultaneously not using naming conventions for resources that make much sense (and are enumerable). In addition, using Software Defined Networks (SDN) is already proving useful to splice connections from original source to original destination and both increase visibility dynamically[18] (think lights going randomly on and off at night versus a prowler), and change the topological appearance to an adversary through traffic breaking and dynamic reroute.[19]

6.5. Cost to Protect vs. Cost for Losing/To Restore

While never an ideal information security practitioner's answer, it is quite reasonable to look at what it will take to protect something versus its actual value, and its secondary value (both are important here). If the customer data is information that is not under legal or regulatory protection (primary), the cost of protecting it from illegal copying may outweigh the need. If the cost from the court of public opinion on breach is significant (secondary), then the secondary may outweigh the primary. Simply stated: if you are spending more to protect something than it is worth, why is that?

The balance is the essential piece here, and its and the balance is affected by risk tolerance, industry, capability and means.

6.6. Summary: Progress Indicators and Thresholds

Don't confuse hard work with results.[20]

Security efforts need clear progress indicators. In order to truly know what the results are, it is necessary to define the means used to measure them ahead of time, and then monitor them accordingly. Budget is not a success measure for security, nor is headcount, organizational structure, or title. Instead, how fast an adversary can exploit your vulnerability, for how long, and how much it might cost versus protecting become the litmus tests for our own progress.

Recommendations and Conclusions

As an insight to what is working, and how well it is working, the TTPs and indicators provided here give a means to answer the questions: 'what can be done now that tips the scales back in our favor, what will it take to get there, and how can I measure my progress?'

With ICT having such profound effects on a nation's economic and security wellbeing, the question must be answered and it will be different for each country or service that asks it. It must still, however, be answered. Albert Einstein once observed that the definition of 'insanity' was to do the same thing over and over again expecting different results. Our industry can fall into that trap, and by some observables, we are in that trap right now. Our adversaries are more than happy to stack rank our defense teams, going after the weakest, using our practices against us. We cannot afford that outcome.

On a positive note, progress suggests that the advanced practices listed here will be standard soon enough, requiring a refresh or perhaps a brand new paper such as this. We owe it to ourselves to make these practices 'standard,' and to bring that day here faster.

References

[1] Cisco, 2012. Cisco Connected World Technology Report. [online] Available at: <http://www.cisco.com/en/US/netsol/ns1120/index.html> [Accessed 30 October 2013].

[2] Dixon, J., 2008. The Risk of Operating in an Inter-Connected Society. [pdf] Team Cymru, Available at: <http://www.team-cymru.com/ReadingRoom/Whitepapers/2008/risk-interconnected-society.pdf> [Accessed 30 October 2013].
[3] Verizon, 2013. 2013 Data Breach Investigations Report. Available at: <http://www.verizonenterprise.com/DBIR/2013/> [Accessed 30 October 2013].
[4] Infosec Island, 2012. Saudi Aramco Investigation. Available at: <http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html> [Accessed 30 October 2013].
[5] Ibid. 2013 Data Breach Investigations Report.
[6] World Economic Forum, 2013. The Global Information Technology Report 2013. [pdf] Available at: <http://reports.weforum.org/global-information-technology-report-2013/> [Accessed 30 October 2013].
[7] Interviewees that agreed to be referenced by name include : Malcolm Harkins, Intel; Roland Cloutier, ADP; Barry Hensley, SecureWorks; Christopher Fajardo, Blizzard Entertainment; and Phil Venables.
[8] Secunia, 2013. German Country Reports. [online] Available at: <http://secunia.com/resources/countryreports/> [Accessed 30 October 2013].
[9] SANS Institute, 2012. Twenty Critical Security Controls for Effective Cyber Defense, version 4.1. [online] Available at: <http://www.sans.org/critical-security-controls> [Accessed 29 October 2013].
[10] Manadhata, P., 2008. An Attack Surface Metric. Ph. D. Carnegie Mellon University. Available at: <http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/2008/CMU-CS-08-152.pdf> [Accessed 30 October 2013].
[11] Llod, M., 2013. Dark Space: What You Don't Know Can Hurt You. Security Week. [online] Available at: <http://www.securityweek.com/dark-space-what-you-don't-know-can-hurt-you> [Accessed 30 October 2013].
[12] Layers 0 through 7 refers to the Open Systems Interconnection (OSI) model, which connects the physical (layer 0) through the application layer (layer 7) in a network, with everything in between.
Wikipedia contributors. 'OSI Model.' Wikipedia, The Free Encyclopedia. [online] Available at: <http://en.wikipedia.org/wiki/OSI_model> [Accessed 22 October 2013].
[13] Spitzner, L., 2010. Honeytokens: The Other Honeypot. Symantec [online]. Available at: <http://www.symantec.com/connect/articles/honeytokens-other-honeypot> [Accessed 31 October 2013].
[14] Wikipedia contributors. 'List of DNS Record Types.' Wikipedia, The Free Encyclopedia. [online] Available at: <http://en.wikipedia.org/wiki/PTR_Record#PTR> [Accessed 22 October 2013].
[15] Lima, S., 2013. DNS and Advanced Persistent Threats (APT). [online] Available at: <http://www.cloudshield.com/blog/dns-security-expert-series/dns-and-advanced-persistent-threats-apt/> [Accessed 31 October 2013].
Jerrim, J., 2013. Detecting Malware P2P Traffic Using Network Flow and DNS Analysis. Damballa Inc. [pdf] Available at: <http://www.cert.org/flocon/2013/presentations/jerrim-john-detecting-malware.pdf> [Accessed 31 October 2013].
[16] Villeneuve, N., and Bennet, J., 2012. Detecting APT Activity with Network Traffic Analysis. Trend Micro Incorporated [pdf] Available at: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf> [Accessed 31 October 2013].
[17] Author's note: one of the leaders in Dwell Time is Jeff Brown and other colleagues at Raytheon, who introduced me to a new way of looking at this particular metric.
Marra, S., Hassell, S., Eck, C., Moody, J., Martin, S., Ganga, G., Harvard, K., Rickard, E., Sandoval, J., and Brown, J., Cyber Resiliency Metrics for Discussion. Raytheon [pdf] Available at: <http://bbn.com/resources/pdf/whitepaper_CyberResiliencyMetricsMASTERv4.pdf> [Accessed 31 October 2013].
[18] Groves, R., and Benetti, B., 2013. Microsoft's Demon: Datacenter Scale Distributed Ethernet Monitoring Appliance. Microsoft [pdf] Available at: <http://sharkfest.wireshark.org/sharkfest.12/presentations/A-4_Leveraging_Openflow_to_create_a_Large_Scale_and_Cost_Effective_Packet_Capture_Network.pdf> [Accessed 31 October 2013].
[19] Heckman, K., 2013. Active Cyber Network Defense with Denial and Deception. [video] CERIAS Seminar: Purdue University. Available at: <http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/flash/6ptedmqa1kgtk3au4jmiplp0v8> [Accessed 31 October 2013].
[20] Fortune 50 CEO.

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-43

Beyond Perimeter Defense: Defense-in-Depth Leveraging Upstream Security

DAVE MCMAHON
The SecDev Group

Abstract. Cyber threats are now so pervasive, sophisticated, and targeted that traditional, reactive computer network defense is no longer sufficient to counter them. Upstream security, which represents a new layer of safeguards that can be deployed well beyond the enterprise perimeter, intercepts malicious activity before it reaches an organization's network. Telecommunications providers are well positioned to offer this type of proactive cyber defense and defense-in-depth, as they possess significant technical capabilities and a unique view on traffic flow. Together, these assets can create a security layer that may operate at higher efficiencies and effectiveness than any enterprise security program. The evidence demonstrates that upstream security and upstream intelligence provide innovative and effective techniques for network defense.

Keywords. Cyber security, defense-in-depth, infrastructure defense, network traffic analysis, proactive cyber defense, telecommunication providers, upstream intelligence, upstream security.

Introduction

This article examines the role of upstream security in cyber network defense-in-depth, illustrating how upstream intelligence can provide enhanced situational awareness (SA) and build a strategic common operating picture (COP). Ultimately, using a proactive strategy vis-à-vis using upstream security can halt malicious activity before it reaches an organization's network.

The first half of the paper reviews the principles of defense-in-depth and offers an explanation of how they should be applied to the cyber domain. It establishes that the concept of layered defense is sound, but needs tuning. Then, it builds the business case in favor of a new upstream layer of security based on the intelligence about the advanced capabilities of adversaries, and the vulnerabilities and limitations of traditional Computer Network Defense (CND). The second half outlines the contours of the solution, covering the current status of the technology available and how it is differentiated, and offering recommendations, technical steps, and concluding takeaways.

1. Principles of Proactive Network Defense-in-Depth

The principle of defense-in-depth[1] is a well-understood military strategy played out on the conventional battlefield to:

- Thwart breaches, by combining effective command, control, computers,

intelligence, surveillance and reconnaissance (C4ISR),[2] mutual coverage, and interlocking arcs-of-fire;
- Impede the progress or maneuverability of an adversary by using heterogeneous[3] obstacles or safeguards, while enabling maneuver and fire for friendly forces; and
- Degrade the enemies' fighting-effectiveness by forcing them to react in a predictable fashion.

When applied to a computer network, the concept of defense-in-depth typically focuses on managing threats inside the organization by segmenting networks into security zones bounded by traditional security appliances at the demarcation points. This classic interpretation of defense-in-depth as applied to a computer network is incomplete for several reasons:

1.1. It is Reactive

CND systems array their sensors inward, as if troops were deployed looking backward into their own lines rather than towards those of the enemy. In this case, sensors need to be placed outside the organization's perimeter and looking in all directions to detect enemy movements, and signals of a preparation-to-attack and traffic egressing from the organization from otherwise undetected compromises. By contrast, a proactive strategy[4] applies defense-in-depth tactics that detect and engage the adversary as early as possible and at a distance, before the enemy can reach and breach the organization's perimeter. Examples from the physical battlefield include: long-range reconnaissance, patrols, vanguards, strategic interdiction, deception, and drones, etc. In the context of computer network defense, cyber-C4ISR can mine global threat intelligence from conflict networks and carrier-level sources, thereby engaging emerging cyber threats in the cloud, upstream of, and external to, the organizational infrastructure. This needs to be accompanied by a willingness to conduct proactive, pre-emptive operations (P2O) in cyberspace to shape users behaviors and avert the development of malicious intent. Direct-action, when required as a solution, will need to be global and coordinated across critical sectors and boundaries.

1.2. It Assumes a Distinct and Hardened Network Perimeter that is not Actually There

The notion that a well-defined and hardened network perimeter exists is a dangerous illusion. The reason for this is straightforward: the layers, components, applications, and processes of an enterprise infrastructure are manufactured, maintained controlled, owned, and operated by many players—some of whom are adversaries. Due to, among other factors, extending supply chains, the evolution of cloud computing, and the proliferation of mobile devices, friendly and hostile infrastructure coexists and co-mingles on the electronic battlefield.

1.3 It assumes that Traditional Security Measures are Effective Weapons against Advanced Persistent Threats despite Evidence to the Contrary

A review of related defense information technology security programs and expenditures demonstrates that the current practice of CND has focused almost exclusively on reactive perimeter defense, zoning, incident response, and disaster recovery.[5] As a result, traditional CND doctrine fails to be informed, to occupy high ground, and to provide flexibility. For example, firewalls are often cited as the preferred solution, despite their questionable effectiveness. Firewalls are inadequate because nearly every organization needs to receive e-mails and web traffic, and attacks today are socially engineered through these vectors. Unlike the rapidly evolving threats it faces, a firewall cannot maneuver or adapt easily. Commonly-used products are proving inadequate to address the next generation of cyber threats, barely providing a Maginot-line type security that merely funnels actors towards more vulnerable pathways. Detecting the presence of malicious actors is challenging, but possible. It requires a different view of security – one that leverages the principles of the large-scale meta-data analysis for detecting weak signs of compromise, and uses techniques such as dark space analysis and a proactive defense against emerging threats. An upstream security layer, informed by global threat intelligence, derived from strategic carrier-level sensors, open-sources, social media, and conflict networks, represents the new arsenal required for CND in this decade. Carrier-level security also allows regulatory authority and national law to provide a full-spectrum of responses against challenges, whether criminal, military, espionage, or otherwise.

1.4. It Equates Abstract Security Zones to Effective Defensive Layers

The concept of zones[6] definitively segments the networking environment into public, public access, operations, and restricted zones, whilst ignoring the space outside the notional perimeter. Furthermore, zones are vulnerability-centric and less relevant from a threat perspective, particularly when addressing the prevalence of cross-domain/blended threats. The reality is that we are providing perimeter defense in one zone from all directions. The shift in thinking is akin to adjusting cold war military doctrine to that of unbounded irregular warfare.

1.5 It does not Inform Defensive Mechanisms with Cyber-C4ISR

Most operators have poor visibility into the threat-ecosystem beyond the walls of their buildings.[7] Modern militaries need accurate and timely intelligence to function, otherwise troops may end up shooting at anything that moves. The same applies to security measures. Strategic assets can produce rich adversarial intelligence that can be actioned tactically. Hence, cyber-defenses should also leverage the cyber-equivalent to strategic C4ISR. Upstream intelligence is part of the solution. It aggregates security metrics at the level of the carrier, commensurate with national jurisdictions, and allows for the detection of weak signals that are otherwise not visible on individual enterprise-level networks. Successful organizations in a competitive environment are those that can disseminate accurate, actionable, and timely intelligence to the front lines of their organization – a truism in both warfare and business.

Operationally, upstream intelligence feeds carrier-level security controls, perimeter defenses, and internal security measures down to edge devices, in real-time. At the strategic and tactical levels, intelligence-led operations can facilitate an organization's capacity to shape its situation,[8] develop opportunities, maneuver in a highly contested space, avoid risk, plan strategically, and forecast accurately, allowing it to achieve a sustainable competitive advantage.

Establishing a clear common operating picture (COP) using upstream intelligence is central to the formulation of a cyber defense strategy for NATO.

Bottom Line: the 'cyber-warrior' needs to rise above the fog of war with actionable intelligence, be agile in the dynamics of irregular warfare, and maintain contact and battle momentum.

2. Systemic Vulnerabilities of Traditional CND

Internal security policies never survive first contact with the enemy

Traditional security has proven ineffective both at detecting and mitigating advanced persistent threats.[9] Users have limited visibility into the threat ecosystem beyond the walls of their buildings—they are short-sighted. As a consequence, most organizations can only see a fraction of how much their network has been compromised by sophisticated malware.

This traditional approach to network security lacks the real-world context required for predictive threat assessments. It falls short of delivering the intelligence necessary to predict and interdict an attack before it occurs. The time lapse between zero-day exploits infiltrating a network and anti-virus signatures detecting the infection represents a considerable blind spot.

Furthermore, there is a very weak correlation between compliance audits, standards, certification, and accreditation, and the volume of malicious activity occurring on a given network. Consequently, relying on policies, standards, and traditional threat-risk assessments to forecast or stop an attack, is much like consulting the farmer's almanac to predict severe weather events and responding to a hurricane with an umbrella. Reacting to an incident after the fact and performing post-mortem disaster recovery is untenable when cyber attacks can occur in stealth and at the speed of light.

In addition, having spam and malware delivered to your perimeter is not only wasteful, it also greatly increases the risk of infection. The transport costs associated with lost bandwidth attributed to toxic content alone justify cleaning the pipes upstream of your enterprise. Organizations should demand 'clean pipes' through contractual mechanisms and standards as a matter of best practice.

No organization can absorb or filter the size of DDoS attacks today except a telecommunications carrier. Moreover, it is more efficient to cut the command-and-control channel of a million-machine botnet upstream at the early stages, than wait for antivirus software to send alerts about compromised computers.

3. Adversarial Rationale

The argument for traditional CND is driven primarily by the threat. On the other hand, the advanced threat calls for upstream security based on the following principles:

- Robot networks (botnets) or trojanized malware are able to deliver measured strategic real-world effects.[10]
  Currently, the annual costs of cyber attacks to private and public sector organizations rival the entire defense budget of some NATO member states. Indeed, widespread attacks and measurable losses are affecting all critical public and private sectors.
- Cyber threats have evolved beyond malicious hackers, script kiddies, and web defacements.
  They now encompass organized crime cartels operating sophisticated robot networks in tandem with hostile foreign intelligence services (HFoIS) and militaries.[11] Attacks are becoming more sophisticated, targeted, dangerous, and undetectable by traditional means.[12] Recent studies confirm that incidents are more frequent and are evolving faster than definitions can be drafted. For example, McAfee's second annual critical infrastructure protection report notes that *'Foreign governments preparing sophisticated exploits like Stuxnet, cyber attackers have targeted critical infrastructure. Hostile government infiltration of their networks achieved staggering levels of success.'*[13] In addition, a study commissioned by the Canadian Government concludes that '*there is an overwhelming quantity of empirical data from upstream network sensors that would suggest a high-degree of penetration, compromise and loss in all the organizations we investigated. None had the necessary strategic security infrastructure, or tradecraft to detect the majority of penetrations to mitigate risks in real-time beyond current levels.'[14]*
- The costs are staggering.
  An estimated 5-12% of computers worldwide are compromised as part of a criminal/spy robot network or botnet. Bell Canada and Secdev research counted 528 billion illicit or malicious e-mails in 2011, or 98% of all e-mails sent that year.[15] Malicious traffic accounted for a whopping 200 petabytes of the sample set, causing an estimated $100 billion in damage. To put this in perspective, 50 petabytes represents the entire works of humankind, from the beginning of recorded history, in all languages. Consequently*, 'persistently changing and evolving threats and threat agents are driving up risks and elevating the need for new security capabilities to counter new risks.'[16]*
- Upstream security is required because traditional Defensive Computer Network Operations (CNO), and traditional IT security, policy, standards, and doctrine are rapidly losing their effectiveness.
  Like global warming, the early-warning signs of impending doom have gone unheeded. The NATO picture may be distorted by a projection of our own constrained offensive capabilities, organizational boundaries, sparse fiscal investments, and legal constraints, onto an adversary that shares none of these restrictions. For example, telecommunications carriers, which are seen as a commodity by many in the West, are considered as strategic military assets by many of our competitors. US and EU commercial assets have already suffered serious predation from Chinese military assets and commercial assets operating under military direction. '*Shifting from 'passive' to active cyberwarfare, the PRC intends to be able to win an 'informationized war' by 2050.*'[17]

4. Strategic Relevance of Upstream Security

'You can't manage what you don't measure.'[18]

Cyberspace is a complex, non-deterministic eco-system similar to global weather patterns or biological ecosystems. Computer networks have been historically managed like office equipment as opposed to weapons-platforms. Similarly, the cyber security discussion has been dominated by techies and policy folks. We require poly-disciplinary teams of social scientists, engineers, computer scientists, operational researchers, and operators able to conduct cross-domain analytics. Competing in cyberspace also requires building an accurate Common Operating Picture (COP), and a keen perception of an organization's attack-surface from the adversary's vantage point, not that of the auditor. This is not possible within traditionalist views of computer network security that rely on internal network health monitoring, doctrine, and policies to define the battlespace.

An upstream security and intelligence capability, on the other hand, addresses the root challenge of cyber warfare—that is, the resilience of critical digital infrastructures. Multiple national capability priorities, including situational awareness, e-sovereignty (national awareness, influence, control, and jurisdiction in cyberspace), threat characterization, and attribution, are achieved by visualizing living infrastructures quantitatively and at scale. In this regard, upstream security and intelligence have been highly effective in identifying present and emerging risks to national infrastructures, and recognizing significant perceptual gaps between internal parochial measurements and external strategic ones.[19]

5. The Solution

5.1. Program Definition

Modern cyber threats can only be countered with next-generation security architectures that are consistent with net-centric warfare and proactive defense-in-depth.[20]
For example, trials in a major telecommunications company demonstrated that proactive cyber defense was the most effective strategy within a real-time integrated risk framework. This proactive approach saved the company over $1 billion per year by detecting and cleaning traffic using upstream security and intelligence.[21] Next-generation security architectures pave the way to deter, detect, and defend against sophisticated future threats. In this regard, telecommunications providers have a unique role to play in mutual CND. These providers occupy the high-ground (control points) at the nexus of both physical and information global infrastructure, within a national framework.

A proactive defense-in-depth strategy necessarily requires a layer of security and intelligence that is deployed upstream of an organization. This strategic capability detects and mitigates attacks and cleans toxic content heading towards the organization or emanating from it. In short, the proactive strategy addresses the threat early and efficiently. Waiting to react to an attacks until it has breached the perimeter, by contrast, is precarious and leaves one with few—and costly—options.

In cyberspace, the carrier is the queen of the battle and should be used in a

military's first line of defense; strategic listening, and force projection.[22] The bulk of malicious traffic (toxic content) can be stopped proactively using techniques like recursive DNS_analytics, stopping the malicious activity before it reaches an organization by invoking upstream security controls deployed at choke points or cleaning centers. It is far safer for an organization not to handle large volumes of toxic content themselves, for reasons of safety and cost-effectiveness. Offloading toxic clean-up and transferring risk to the upstream provider frees the organization to divert its security budget towards tackling unique problem-sets, insider threats, and mopping-up what attacks actually get through. The risks for organizations caught in the crossfire of a malicious attack are not a new or unknown issue.[23] Doing something about it requires adjusting the rules of the road, including revisiting telecommunications regulations. Such a task will not be easy. The telecommunications industry may be highly regulated, but it is also subject to multiple competing interests from operators, vendors, and interest groups. Changing the status quo will require significant political will, and a willingness to expend political capital. Few governments have the stomach for this fight.

5.2. Current Status of the Technology

The current technical environment presents unique challenges for network security. Interoperability, the globalization of supply chains, and extensive outsourcing have lowered costs, but have also increased dependencies, making many of the underlying features of security reliant on trust. Moreover, information technologies are by definition dual use and whereas G8 countries have traditionally used export controls to prevent technologies from being weaponized or used in ways that are inconsistent with international norms, that has not always been the case. Nation states, at times working hand-in-hand with organized crime and other groups, have demonstrated an ability to appropriate and engineer Western technologies to suit their strategic needs. This ranges from repurposing Deep Packet Inspection (DPI) and Internet filter appliances, to enforcing national censorship, to using equipment intended for mass surveillance and intelligence gathering against groups within, and outside national borders.

Supply chains also represent a risk. National telecommunications providers buy pieces of equipment globally, often without considering the risks and vulnerabilities of how access to these technologies could be exploited by nation-states, organized crime groups, or other malicious actors.

Cyber deterrence will be called upon to mitigate cyber threats to national security, critical infrastructures, supply-chains, and economic prosperity, until technical advances will allow for better hardening and resilience against advanced persistent threats and full-spectrum cyber war.

Achieving such technological advantage and resilience will be difficult, as it requires applying export controls in ways that restrict bad actors from exploiting dual-use technologies for offensive means. This may mean choosing not to export some technologies abroad. This will also require establishing international norms governing trade in dual-use cyber technologies. Otherwise, the risk is to lock out G8 companies from competing with countries that feel no compulsion in restricting export of technologies built for surveillance and censorship. Likewise, applying due diligence to supply chains will be difficult, as it runs against the commercial interests of operators already competing in a crowded and competitive market space. Equipment costs are the major investment for telecommunications providers, and they will most likely be

reluctant to buy national brands if this significantly increases their operating costs vis-à-vis competitors who do not have the same restrictions.

At the same time, cyber deterrence using strategic-power can help address non-state actors engaged in nascent cyber terrorism, rampant cyber crime, and growing international black markets for malware and offensive tradecraft. In this respect, carrier-upstream can influence malicious actors on multiple levels:

- *Technical* – as owner-operators of the network can control content and routing.
- *Physical* – traffic is consolidated within facilities controlled by the Telco.
- *Market* – all actors (good and bad) benefit from the goods and services offered by telecommunications providers. Conversely, carriers will provide the security the market demands.
- *Regulation* – the industry is highly regulated, albeit price and ownership focused. A certain baseline security standard could be instituted as a condition of licensing.
- *Standards* – are driven by suppliers and primary buyers of information communications technology.

The research, science, and technology currently exist to support such initiatives.[24] Upstream security and intelligence services have been productized for over a decade, but neither technology nor costs have been the principal impediment to successful proactive cyber defense programs involving upstream security. The major challenges to defense strategy appear to have been a lack of an organizational behavior models, mission ambiguity, legal and privacy speculation, doctrinal hurdles, and perceived information sharing concerns. The roll-out of commercial upstream defense capabilities, products, services, and intelligence by the private sector has been further delayed by intellectual property protection, cost recovery, and nascent market demand.

More recently, a fusion of upstream security and intelligence with open source intelligence and social media analytics has shown to be highly promising in providing vital socio-political context to network metrics, and in closing the attribution-chain on attackers.

5.3. Technology Differentiation

Upstream security is distinct from traditional CND in that it is strategic, proactive, and global, offers defense-in-depth (external to internal reach), and is cost-effective.

Quantitative market analysis of IT security procurement shows that organizations overwhelmingly purchase tactical point-solutions in the form of patchworks of expensive, reactive, static, internally-facing appliances, and software designed to appease policies, rather than systematically addressing a rapidly evolving threat. IT security risk decisions are thus typically driven by audits, not by science or intelligence.

Our adversaries prefer to lead with strategic offence and pro-active defense from within highly agile synthetic intelligent networks, cloaked and anonymized, and are tuned towards espionage, fraud, influence operations, and disruption.[25] To win the engagement in cyberspace, militaries need to transition from ‘closed’ fortress networks, towards secure agile networking and cloud technologies, with upstream security in direct support.

Recommendations and Conclusions

The following are recommended technical measures based on their high-protective index and cost-effectiveness,[26] and calculated by the quantity and severity of malicious traffic that is detected, blocked or avoided per dollar spent:

- Recursive DNS analytics to detect and mitigate malicious traffic behavior on root organizational domains;
- Dark space, conflict networks, and honeypots to detect zero-day exploits and APT;
- Sanitized security metadata from trusted carriers for upstream security;
- Fusion of open source/social media analysis to prepare the electronic battlefield for real-world context and attribution;
- Formation of poly-disciplinary teams of social scientists, engineers, computer scientists, operational researchers, and operators to conduct cross-domain analytics;
- The use of validated upstream reputation ratings that can be applied down to traditional security appliances or software;
- Subscription to 'clean pipes' through contractual mechanisms and standards as a matter of best practice;[27] and
- Adoption of agile secure networking in the cloud.

This is a summary of additional practical recommendations, which have been highlighted throughout this paper:

- Use cyber-C4ISR to mine global threat intelligence from external sensors, conflict networks and carrier-level sources;
- Leverage the principles of large-scale meta-data analysis for detecting weak signs of compromise;
- Use upstream intelligence to provide a more global threat picture, create blacklists, reputational ratings, and threat signatures, and program traditional security appliances and end-device software;
- Fuse upstream security and intelligence with open source intelligence and social media analytics to provide socio-political context to network metrics, and close the attribution-chain on attackers;
- Train the next generation of poly-disciplinary teams of social scientists, engineers, computer scientists, operational researchers, and operators able to conduct cross-domain analytics, and include them in the cyber security discussion; and
- Urge militaries engaged in cyberspace operations to transition from 'closed' fortress networks towards secure agile networking and cloud technologies, with upstream security in direct support.

As highlighted throughout this volume, networks have gone global, and there is no longer a clear perimeter. Most of the infrastructure we used to know is now in the cloud or has been globalized. Access to big data is necessary to detect APT, and attribution requires cross-domain analytics using social media, although only Tier 1 Carriers are able to address nation-crushing Distributed Denial of Service (DDoS) attacks. Therefore, perimeter security is a lot like a installing a screen door on a submarine, and relying on end-point solutions to act as bilge pumps.

Upstream security represents a new layer of safeguards that can be deployed well

beyond the organizational perimeter, at the carrier-level, and from the Internet at large. This layer yields high-efficiencies and new capabilities not available to an enterprise security program. Upstream security both creates and draws upon core intelligence to provide a more global threat picture, create blacklists, reputational ratings, and threat signatures, and program traditional security appliances and end-device software. The combination of upstream security and intelligence can provide both defense-in-depth and proactive defense, which can engage the threat at a distance and degrade the attack. There are strong business cases and mature technical solutions available to organizations to implement upstream computer network defenses.

Finally, network fortresses will find themselves victims of siege tactics and are no match for an asymmetric enemy practicing maneuver warfare at the speed of light. Agile, secure, cloud-based infrastructures represent the future, together with upstream security and intelligence providing the strategic air cover.

References

[1] Wikipedia contributors. 'Defense in depth.' Wikipedia, The Free Encyclopedia. [online] Available at: <http://en.wikipedia.org/wiki/Defence_in_depth> [Accessed 22 October 2013].
[2] US Department of Defense. Department of Defense Architecture Framework (DoDAF). Washington, DC 2010.
[3] Heterogeneous safeguards require different attack vectors, as opposed to the same type or brand of security control deployed in a row that can all be compromised by the same exploit.
[4] A proactive cyber defence doctrine compels an organization to act by interdicting and disrupting an attack pre-emptively in self-defence, in order to oppose the attack against their computer infrastructure. Defending-in-depth ensures that engagement with the threat occurs at a safe distance in time and space.
[5] In 2010, Bell Canada and Secdev Group were tasked by the Department of National Defence to gather military procurement details, through proactive disclosure and cross-referenced industry statistics, in order to contrast military expenditures with strategic IT security plans and protective index.
[6] Government of Canada, Communications Security Establishment Canada, 2009. Information Technology Security Guideline (ITSG-38) Network Security Zoning. [online] Available at: <http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg38-eng.html> [Accessed 22 October 2013].
[7] Bell Canada and the RAND Corporation, 2006. Cyber Critical Infrastructures Interdependencies Study 0D160-063075/A, Public Safety Canada.
[8] 'In a world where threats can change minute to minute, and security posture changes at the same rate, open source information ranging in age from hours to days or weeks only begins to address the enterprise needs for cyber threat intelligence.' Macaulay, T., 2010 Anatomy of Upstream Intelligence. IA Newsletter, 13(3), p. 26.
[9] McMahon D., and Rohozinski, R., 2010. Combating Robot Networks and Their Controllers. Bell Canada and SecDev Group. [online] Available at: <http://publications.gc.ca/collections/collection_2011/rddc-drdc/D66-4-2009-eng.pdf> [Accessed 22 October 2013]; and McAfee, 2011. Global Energy Cyberattacks: 'Night Dragon.' Santa Clara, CA: McAfee, Inc. [online] Available at: <http://www.mcafee.com/ca/about/night-dragon.aspx> [Accessed 22 October 2013].
[10] The Information Warfare Monitor Project, 2012. The Dark Space Project. Combating Robot Networks and Their Controllers Study. Global Energy Cyberattacks: 'Night Dragon.' Aurora. Koobface: Inside a Crimeware Network. Shadows in the Cloud: Investigating Cyber Espionage. McAfee Annual Threat Report. GhostNet. [online] Available at: <http://www.infowar-monitor.net/> [Accessed 4 November 2013].
[11] Glenny, M., 2008. McMafia: A Journey Through the Global Criminal Underworld. 1st ed. London: Bodley Head; and Glenny, M., 2011. DarkMarket: Cyberthieves, Cybercops and You. New York: Knopf Publishing Group.
[12] Ibid. Global Energy Cyberattacks: 'Night Dragon.'

[13] Baker, S., Filipiak, N., and Timlin, K., 2011. In the Dark: Crucial Industries Confront Cyberattacks. Santa Clara, CA: McAfee, Inc. [online] Available at: <http://www.mcafee.com/cip_report> [Accessed 22 October 2013]
[14] Ibid. The Dark Space Project.
[15] The fact that 94-98 % of email is spam is a widely quoted figure from Microsoft, McAfee, Symantec, Trend Micro et.al. Independently verified by Bell Canada and the Secdev Group. Study on the Analysis of Darknet Space for Predictive Indicators of Cyber Threat Activity, 2011. Public Safety Technical Program, Centre for Security Science, Defence Research Establishment, Secdev, Bell Canada, Communications Security Establishment of Canada (CSEC), Royal Canadian Mounted Police (RCMP), Department of National Defence (DND), Canadian Security Intelligence Service (CSIS), Canada Revenue Agency (CRA), and Industry Canada (IC), McAfee.
[16] Macaulay, T., McMahon, D., and Mac-Stoker, C., 2010. Upstream Intelligence and Security Series: Delivery Options for Upstream Intelligence, Upstream Intelligence in the World of Legal Compliance and Liability, Upstream Intelligence: A New Layer of Cybersecurity, Anatomy of Upstream Intelligence, Business Models of Upstream Intelligence Management and Distribution. Information Assurance Technology Analysis Center (IATAC), Department of Defense (DoD) managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E).
[17] Housworth, G., 2007. Informationalization in Chinese military doctrine affects foreign commercial and military assets. Gordon Housworth Community Weblog, [blog] 31 May. Available at: <http://spaces.icgpartners.com/index2.asp?NGuid=E2605D41B8DC46A58813E69E976EC8A1> [Accessed 22October 2013].
[18] Deming, W. E., Plan-Do-Check-Act.
[19] Ibid. Cyber Critical Infrastructures Interdependencies Study
[20] Defense-in-depth strategy means engaging and maintaining contact with the threat at a distance (external to the organization) starting with the notion of 'clean-pipes' and upstream security, and maintaining contact (if necessary) from the perimeter inside the organization.
[21] Ibid. Combating Robot Networks and Their Controllers.
[22] Rohozinski, R., 2013. Commentary at the Conference on International Engagement on Cyber. Georgetown University, 10 April 2013.
[23] Indeed this was argued convincingly in a 2009 MacAfee report: 'As long as major governments desire unimpeded operational freedom in cyberspace, it will continue to be the Wild West. In the meantime, the owners and operators of the critical infrastructure, which makes up this new battleground will continue to get caught in the cross-fire.' Center for Strategic and International Studies (CSIS), 2009. In The Crossfire: Critical Infrastructure in the Age of Cyber War. Cyberwar Resources Guide (158). Santa Clara, CA: McAfee, Inc. [online] Available at: <http://resources.mcafee.com/content/NACIPReport> [Accessed 23 October 2013].
[24] '… network service provider is best suited to provide security services. There are numerous reasons for this: a) The network generates data that can be profiled and analysed for anomalies that may be leading indicators of threats that are developing on the Internet. A large network service provider has a good vantage point to identify new threats and incorporate mechanisms to counteract them well before most network users can see them. b) Providers of private enterprise services can analyse the same types of data for both internal and external threats. Their customers can minimize their need to implement separate internal network protections to supplement Internet gateway solutions. c) Many providers control huge amounts of bandwidth in the core network where flooding attacks can be routed away from smaller bandwidth customer access links.' Interview with Brian Rexrod, Principal Network Security Architect at AT&T Chief Security Office, by General Clive Addy. FrontLine Security Magazine, Spring 2010.
[25] Ibid. Combatting Robot Networks and their Controllers
[26] Ibid. The Dark Space Project.
[27] 'Better Bandwidth Utilization with Network-based Defence - By removing attack traffic within the IP backbone, the Internet Clean Pipe solution rapidly clears threats in the cloud before they hit the customer network. The solution also provides users with multiple bandwidth speeds and ensures optimal bandwidth usage. Proactive, Real-time Mitigation [are] built into a global IP backbone for full transparency to users once mitigation begins. The service scrutinizes network traffic in real-time to identify anomalies and quarantine attack packets. Only malicious traffic is blocked — legitimate traffic continues to flow through so network and applications remain available to users.' TATA Communications, 2009. Internet Clean Pipe - DDoS Protection: Global Tier-1 network with built-in DDoS Detection and Mitigation services. [online] Available at: <http://www.tatacommunications.com/downloads/enterprise/Data%20Sheet%20-%20%20Internet-clean-pipe%20-%20DDOS%20Protection.pdf> [Accessed 23 October 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-54

Back to Basics: Beyond Network Hygiene

FELIX 'FX' LINDNER[a] and SANDRO GAYCKEN [b]
[a] *Recurity Labs GmbH, Germany*
[b] *Freie University of Berlin, Germany*

Abstract: In the past, Computer Network Defense (CND) intended to be minimally intrusive to the other requirements of IT development, business, and operations. This paper outlines how different security paradigms have failed to become effective defense approaches, and what the root cause of the current situation is. Based on these observations, a different point of view is proposed: acknowledging the inherent composite nature of computer systems and software. Considering the problem space from the composite point of view, the paper offers ways to leverage composition for security, and concludes with a list of recommendations.

Keywords. Building blocks, cyber defense, cyber security, decentralized public key infrastructure, full stack security, Harvard architecture, information flow control, LangSec, micro kernels, moving targets, separation kernels, verification process.

Introduction

Defending computer networks can appear to be an always losing position in the 21st century. It is increasingly obvious that the state of the art in Computer Network Defense (CND) is over a decade behind its counterpart Computer Network Offense (CNO). Even intelligence and military organizations, considered to be best positioned to defend their own infrastructures, struggle to keep the constant onslaught of attackers with varying motives, skills, and resources at bay. Many NATO member states leave the impression that they have all but given up when it comes to recommending effective defense strategies to the entities operating their critical national infrastructure and to the business sector.

At the core of the problem lies a simple but hard historic truth: currently, nobody can purchase secure computer hardware or software. Since the early days of commercial computer use, computer products, including the less obvious elements of the network infrastructure that enable modern use of interconnected machines, have come with absolutely no warranty. They do not even promise any enforceable fitness for a particular purpose. Computer users have become used to the status quo and many do not even question this crucial situation anymore.

The complete lack of product liability was and is one of the driving factors of the IT industry as it fosters a continuous update and upgrade cycle, driving revenue. Therefore, no national economy that has any computer or software industry to speak of can afford to change the product liability status quo. Such a change would most likely exterminate a nation's entire IT sector immediately, either by exodus or indemnity claims. The same economic factor caused the IT industry to focus research and development efforts on functionality aspects of their products, adding more and more

features, in order to support the sales of the next version of products. Simply put, there is no incentive to build secure and robust software, so nobody does it.

Over time, we have built an IT landscape which consists of many rotten building blocks. Gerald M. Weinberg's Second Law is often quoted: 'If builders built buildings the way programmers write programs, then the first woodpecker that came along would destroy civilization.'[1] When it comes to CND, this situation is aggravated by the fact that so-called security software—the very building blocks that we try to use for our defenses—are, by far, of worse quality than anything else.[2] Statistically, not actually using it would be more secure.

This paper will explore what does and does not work in defense, and discuss how we can reduce the defense problem to a building block problem.

1. Composition – Why Basics Matter Most

Computer systems are, like many other things in engineering, constructed by composition. The same actually holds true for attacks (so-called exploits), which are composed of software flaws and incorrect functioning of pieces on the victim's side. This creates a Weird Machine[3] on the victim's system that allows the attacker to do what he wants.

From a security point of view, the composition of computer systems is a crucial feature. It reaffirms that any IT-system is, in fact, not just one system, but a heterogeneous multitude of systems, with many different facets and properties, a variety of relations and entanglements with one another, and – by now – in constant flux because of continuous updates, structural changes, addendums, and other practices. All these aspects are relevant for security. Put together, they create a formidable problem.

Unfortunately, the composition aspect was, and often still is, ignored by defense approaches. Some of the more common defense approaches will be reviewed in the following sections.

1.1. The Perimeter Security Paradigm

At the end of the 20th century, computer security issues were still considered more of an organizational problem than a fundamental technical one. In hindsight, this was probably more true so a couple of decades ago, when systems were significantly less complex and their building blocks smaller. The dominating principle of UNIX was one of programs that 'do one thing, and do it right.' So the general assumption was that a competent operator of a system could also properly defend it.

The Perimeter Security Paradigm simply describes an organizational approach to limit the exposure of not-so-well administrated machines towards a potentially hostile network. With that in mind, the idea of a handful of firewalls protecting the network was born. On the 'inside,' the fragile building blocks could continue to be used (and more could be added), while the 'outside' had to be prevented from affecting them. In addition, many organizations retreated to the high ground argument that their network is not connected, and hence not exposed, to any hostile network.

This idea is, however, antithetical to the value of having networked computers in the first place. In order to reap the benefits of communication, one must be able to communicate. Accordingly, more and more interconnections were added and the

perimeter simply vanished over the years. Recent trends like Bring Your Own Device (BYOD) are only the final nail in the coffin.

By now, it is clear that the Perimeter Security Paradigm has only delayed a broader recognition of just how vulnerable the building blocks are.

1.2. The Selected Vector Security Paradigm

In a quite similar fashion, computer security developed other focal points at which to implement security. The guiding principle in this case was usually one of minimally invasive measures, applied *ad hoc* to a specific system along with other needs. These measures were applied in a surgical manner to only a very few places, which had been the most common vectors of attacks, so no other 'critical' specified function was disturbed.

This approach, however, is dangerously flawed from the outset. Attackers are not like natural catastrophes. They can analyze their targets for vulnerable elements. Isolating single, selected vectors only shifts them onto a different, less observed, and less protected vector.

An example is encryption. Even today lay people and encryption technology salesmen tend to think that encryption can solve everything—if simply everything could be encrypted, everything would be safe. This reasoning, again, pays little heed to the composite nature of information technology. Encryption can only protect certain content under certain conditions. It will not protect the operating system in charge of the encryption process and in charge of holding the keys. Thus, selling encryption as a critical guard at a critical gate for overall system protection is clearly mistaken, just like any other kind of protection focused on selected vectors. In a composite system, there is no critical gate: everything is a gate.

1.3. The Detection Paradigm

The Detection Paradigm was the next step in defense approaches that completely ignored the composite nature of both computing environments and attacks. Under this paradigm, we subsume all approaches that try to detect attacks, be they anti-virus software, intrusion detection systems, or its more recent sister—intrusion prevention systems.

The basic idea is to detect malicious behavior on the computer system or the network *while* it is occurring. Besides the inherent and well-known flaw in this approach, namely that the malicious behavior must be more or less well known before it can be detected, this approach also fails spectacularly at recognizing the composite nature of attacks. Exploitation frameworks easily demonstrate this,[4] where the building blocks of the attack are composed individually for each attack. Not surprisingly, individually composed attacks are rarely detected by the systems that are deployed for this exact purpose.

On top of that, the situational awareness provided by those detection systems is a worst-case scenario for the defender. If the attack is obvious enough for the system to detect it, it could also be prevented upfront, so no additional benefit whatsoever is achieved. If the attack is only an indicator of something larger going on, the defender is pushed into a real time verification requirement in order to still have a chance to react. Even the later addition of information correlation using Security Information and Event Management (SIEM) solutions, aiming at improving situational awareness, cannot

change this underlying race condition that is almost always a guaranteed losing point for defense.

1.4. The Vulnerability Identification Paradigm

The last of the four paradigms is the idea of attack prevention by reducing the number of known vulnerabilities in computer systems. This approach is about as old as the Perimeter Security Paradigm, but at least it begins to acknowledge that the root cause is flaws already present in computer systems. However, this approach also falls short of taking the composite nature of these systems into account.

Due to the complete lack of legal enforcement measures to compel software vendors to produce more robust and hence more secure software, the Full Disclosure movement was developed. System administrators, software users, and security enthusiasts joined this movement, and started to publicly report identified security vulnerabilities, thereby shaming vendors into fixing them. The movement managed to achieve part of its goal, depending on the respective vendor. Most countries now have both Computer Emergency Response Teams (CERTs) that track the vulnerability information published, and openly accessible databases like the National Vulnerability Database[5] that maintain catalogues of them.

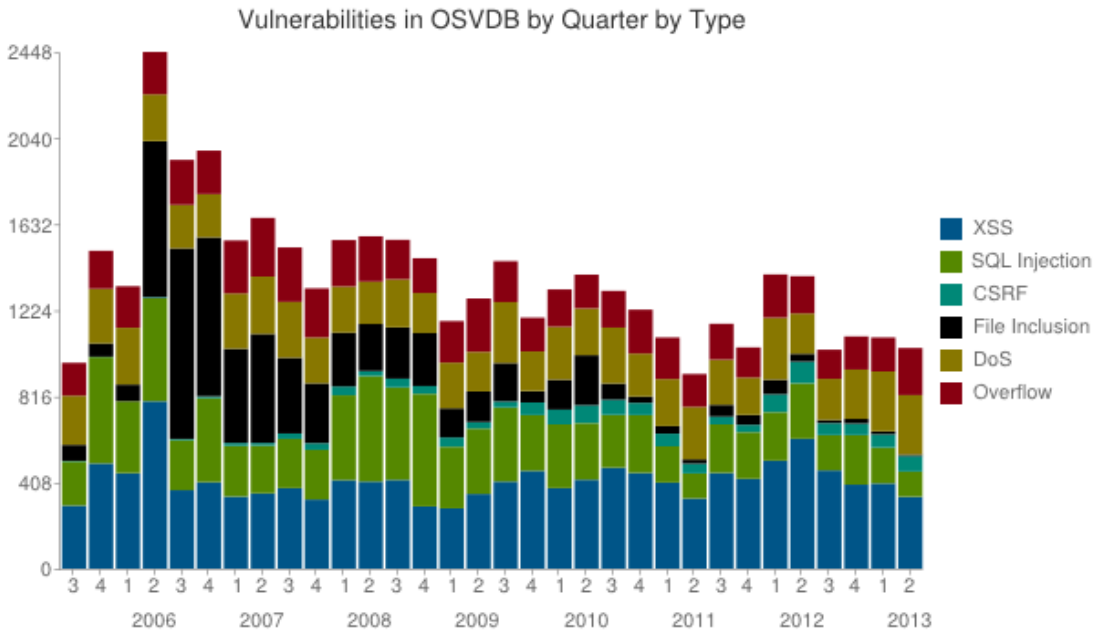


Figure 1: Vulnerabilities in OSCDB by Quarter by Type

Full Disclosure, however, only works as long as the information is coming in. This was the case for a long time, since there was no other legitimate (legal) use for information about security vulnerabilities, other than the modest fame connected with having discovered them, so they were openly shared, but the global rise of nation state CNO operations has created a lucrative market for turning exactly this type of information into attacks, with prices up to $250,000 per item.

While the total number of vulnerabilities reported has been relatively stable over the last decade, our recent research has shown a sharp decline in reports of the type of vulnerabilities considered useful for CNO—namely weaknesses in server software as well as in commonly used desktop client programs, like web browsers. Regrettably, even the overall number of vulnerabilities reported appears to be in moderate decline, which does not correspond to the amount of vulnerabilities actually discovered.

Full Disclosure also drives the development of security patches by the software vendors, at no profit for them. Therefore, reduced public reporting of security vulnerabilities is economically in the interest of the software vendors. Perversely, it is also in the interest of many operating entities, because if vendors do not issue any patches, no systems needs to be updated, and operating costs go down. There is an already discernible push from some software vendors to regulate security vulnerability information, because of the described economic benefits.

The Vulnerability Identification Paradigm, as well as the Detection Paradigm, however, depends completely on the availability of information. Products like vulnerability scanners that inspect computers on the network for known weaknesses are already losing efficiency due to the lack of detail in publicly accessible information. This trend will continue as incentives to keep information under wraps increase, and this defense paradigm is expected to soon lose much of its significance for network security.

Additionally, the Vulnerability Identification Paradigm's failure to address the composite nature of systems often leads to unaddressed issues such as the fact that the vulnerability stems from an interaction between components of a system, especially when these come from different sources. It is easy to see how multiple parties will try to blame everyone but themselves. Another problem is to know how and by whom a component will be used, and what assumptions a user will have.

2. Leveraging Composition for Defense

As outlined above, the composite nature of attacks as well as of the computer systems to be defended should be the focus of any long term future attempts to improve defense posture. The following recommendations offer realistic, economically feasible, and effective approaches to network security.

Although these recommendations are organized from the most general to the most particular, they should be considered as a whole. It also has to be pointed out that they refer to systems built in the future and are not meant to be retrofitted into legacy systems.

2.1. The Prevention-Detection-Recovery Triangle

Efforts in CND have historically been entirely prevention-centric. As understandable as this focus is, it just does not represent the real world. There is no perfect prevention, neither in the fifth nor in any other domain. Future developments need to take into account from the start that attacks will continue to evolve faster than defense can keep pace with, and that current as well as evolved attacks will be successful from time to time.

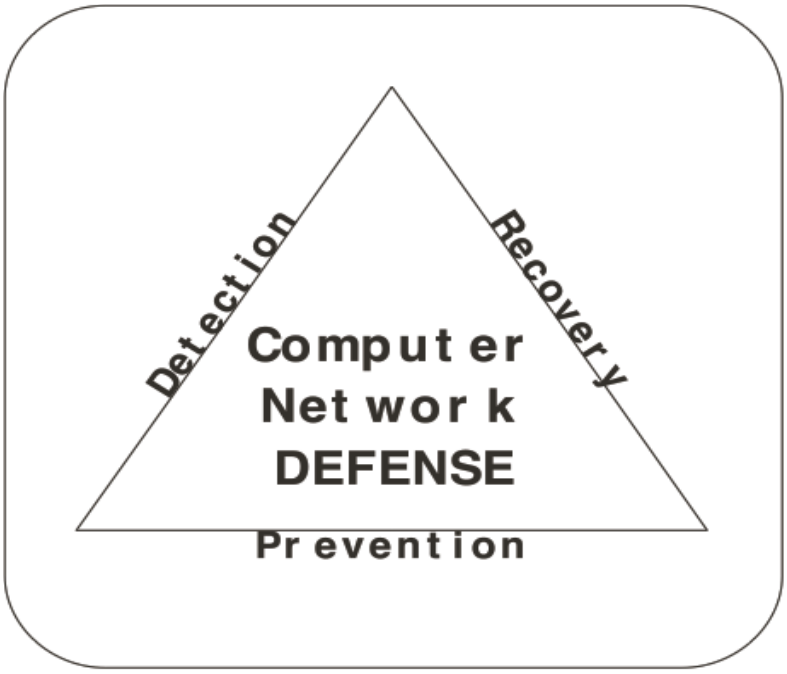


Figure 2. CND Triangle: Prevention, Detection, and Recovery.

Looking at defense in a more realistic manner should also be about detection. This detection, however, has very little in common with what was described above as the Detection Paradigm. It centers on the idea that an attacker loses his advantages the moment the attack is successful. This is also often referred to as the 'defender's home field advantage.' Instead of trying to detect attacks while they are in progress, which has proven not to be very successful, the focus should shift to detecting the intruder once the intrusion has taken place. Post exploitation activity is a relatively long process when concerning valuable targets.[6] New detection approaches should take into account that illegitimate use of computer resources—whether by an insider or an external threat that successfully elevated its privileges into a system—is when the *actual intrusions* can be best identified.

Considering that complete prevention is not possible, and that the capability to detect misuse is independent of concepts like 'inside' and 'outside' threat, leads us to a third element of CND: recovery. Compromised resources can no longer be considered trustworthy in any way. However, in contemporary wisdom, trying to remove the artifacts left by an attack can solve this issue. This practice, however, is rarely successful and only aids future intrusions, because the weakness initially used for the attack is not identified and hence not remedied. The reason for this questionable practice is that today's systems cannot be recovered to their state before an attack due to their sheer size. Reinstalling a single computer after a virus infection is easy, but the same is simply impractical for an Enterprise Resource Planning system (e.g. SAP ERP) or an Industrial Control System (ICS).

Therefore, our first recommendation is to **significantly increase the granularity of the building blocks, making the individual building block significantly smaller** than what is done today.

Interestingly enough, the biggest single building block today, commonly referred to as the Cloud, already makes use of this small building block concept on the resource

layer. Individual host machines as well as virtual machines running on them are small blocks with which actual applications, databases, and distributed storage are built. Detection and especially recovery are greatly improved in the Cloud. The virtual machines can be silently inspected from the hypervisor side and be transparently removed and replaced in case of security concerns.

2.2. Speculative Clean Slate

In another twist of 'back to basics', revolutionary ideas for computer security developed in the past decades should be considered. Many of these ideas would have brought IT-security from its immature and dangerous state to one with satisfactory security and higher standards, but they were never very popular. A major problem was that they were often more costly or less efficient and thus provided no incentive for heightened security, or they did not fit well into the existing legacy of technologies. Many of these ideas, in fact, proposed a 'clean slate' as a condition. Considering that, in the past, security concerns were low to nil, there was no real reason to start any reform of the existing environment despite the fact that virtually everyone knew how vulnerable it was and that the decisions taken were irresponsible. Politics could have enforced these more innovative ideas, but politicians were never tech-savvy enough to make controversial decisions against a larger market mainstream. Therefore, many of the very good ideas about IT-security remained speculative. But this is not to say that they are unrealistic. First, in times of a drastically changing cyber security environment, the top shelf ideas should be revisited. Second, many of these ideas had their own little microevolutions in the computer sciences and have often reached levels of maturity sufficient to be implemented in present-day machinery, without any, or at least without significant, loss in performance. Exploring these ideas more thoroughly should be especially interesting for cyber defense.

These are some examples of these innovative ideas that should be considered:[7]

- Harvard architectures: Basic architectures today are 'von Neumann' architectures, which do not distinguish between data and programs. A switch to 'Harvard' architectures would change this, thus making it much harder for an attacker to redirect code flow into data.
- Moving Target architectures: Architectures could be designed to move around in their configurations, thus confusing attackers and rendering it more likely that their attacks generate problems or detectable patterns, and are discovered.
- Microkernels: These operating systems function with much less code, rendering attacks on the OS-level much harder. Some of these are already at work in aviation.
- Formal specification and verification: Well-understood processes could be better specified, in a formal way, and applications and operating systems of smaller code basis could be verified. This way, processes, applications, and operating systems would be mathematically proven to be correct and without typing errors or buffer overflows and similar faults.
- Separation kernels: These operating systems have functional separations within the kernel, rendering a migration of attacks much harder.
- Information Flow Control: This technique could recognize and disrupt illegitimate data flows.

- Full Stack Security: As a part of the clean slate paradigm, the composite nature of IT-systems should be addressed as well. In all critical systems with serious and resourceful attackers, securing all components is unavoidable in the long run. The whole system and the full stack must be secured. Any vulnerable layer could be used as an access vector onto some or all functions of the system.

Many of these ideas had very interesting approaches and prototypes over the past decades, and have been formulated (though never implemented) as requirements. An example is the orange book, an old standard for the evaluation of computer security which – sadly and strangely – had much tougher views on security in the 80s than today.[8] They must be revisited these days.

Militaries will also have to seriously consider changing some of their present paradigms back to older ones. High Security-IT simply does not work very well in an environment constituted by 'Network-Centric' and by 'Responsibility to Share'. This, to quote a frequent phrase of sci-fi robots (which mostly blow up right after saying it), 'does not compute.'[9] Disconnecting the networks and switching back to more swarm-like, decentralized tactics and strategies, based on carefully engineered versions of 'commander's intent,' is a clear task ahead.

This is not necessarily 'retro.' It invites a continuous use of IT and high tech, only of a different kind and in an entirely different overall structure. We should not forget that those military paradigms have been developed for a reason. The 'Network-Centric' paradigm was invented to allow coordination of a diversity of troops against highly flexible and mobile adversaries. The same could be done with swarm intelligence models, but without the vulnerabilities caused by 'network' and by 'centric' (if done properly!). The 'Responsibility to Share' paradigm was introduced to enable militaries to cope with the overwhelming amount of information available, which they automatically gather in these times of vastly more efficient (and numerous) intelligence and analysis methods. A 'many eyes' principle, having many people look at everything, seems an obvious choice to confront this problem. Yet in a digital environment with uncertain security features everywhere, 'many eyes' almost always include hostile eyes. Recent events have demonstrated as much. But again, the same functionality could be provided by a smarter use of technology. One idea would be to relocate some of the NSA's capabilities in semantic web analysis onto their own semantic web, enabling a digital process of 'many eyes' and, if done properly, disabling malicious and unauthorized users; an insecure semantic web analysis would be a grave single point of failure.

2.3. Protecting Interfaces Using LangSec

The smaller the building blocks are, the more communication is required between them. This is a desirable outcome, since communication interfaces are where security can be most easily modeled, implemented, and enforced. The LangSec movement[10] is a language-theoretic approach to achieve that.

Handling the composition of computing systems is arguably the hardest task of both security theory and practice. A system composed of parts with well-understood properties typically has emergent properties that are hard to derive, validate, or even detect from the properties of the parts. These new properties often come as a nasty surprise, creating vulnerabilities that only manifest when building blocks are combined.

The language-theoretic view of security examines system and program components as computational automata, both in isolation and when combined into larger systems. This approach has led to the discovery of serious vulnerabilities in the X.509 PKI infrastructure, remote physical layer frame injection in 802.11b and other wireless protocols, and attacker-driven computation in the binary programs. Defensively, it also points out the way to better implementing security through message validation, and the conceptual separation of code between input recognition and processing. This field explores how to employ language-theoretic principles to construct software that are robust by design and expose as little state and computational power as possible to adversaries.

The idea is to find a 'sweet spot' between formal software validation and the collective experience of both software exploiters and defenders in the field. Language-theoretic security offers a way to design protocols and build systems that can actually be validated and avoid large classes of bugs. Various success stories in both attack and defense have shown the efficiency of this theory in direct practical application.

While the approach initially sounds theoretical and over-formalized, it is actually of very practical nature. Consider the example of a larger system development project with multiple parties. It is common for communication interfaces to suffer from different interpretations of messages sent between them. This is also where most attacks will bring their pressure to bear, since any misinterpretation can almost always be leveraged for an attack. With the LangSec approach, the parties to a communication will specify simple lists of what the content of the messages will be. Once all parties agree on these requirements, a tool will determine the minimal language complexity class[11] and an appropriate formal grammar, and then generate the program code for all sides involved. The formal grammar can later be used to independently and automatically test whether the integrated version of the program code still fully complies with the specification. Therefore, the approach produces secure and verifiable interfaces while reducing development cost and time.

Another use of LangSec is the creation of normalizers,[12] which reduce language complexity and enforce formal grammar on incoming data in order to protect legacy fragile building blocks that consume their output.

2.4. Decentralized and Fine Granular Trust

Computer Network Defense is not an end in itself. The goal is to obtain and maintain control over functionality and data. However, even with perfectly verified and working systems and networks, it is still of paramount importance to handle identification of people as well as authorization of their activities. This problem space has recently experienced a sharp increase in attention due to insider threats and leaking of classified data.

Authentication and handling of cryptographic key material remains challenging. The case of the Dutch certificate authority 'DigiNotar'[13] has once again demonstrated that hierarchical approaches are too fragile and easy to attack, since the adversary immediately gains control over everything below his intrusion point in the hierarchy, and detection by the affected entities is close to impossible. However, alternative decentralized approaches like ISO 20828[14] have been specified and practical implementations of systems derived from those approaches are under active development.

Agile, decentralized, public key infrastructures (PKI) separate the authentication from the authorization problem, eliminate practical issues like certificate revocation, and provide a graceful migration path from centralized hierarchical infrastructure.

Recommendations and Conclusions

The following steps should be undertaken to reduce risks to the building blocks of our network defense:

1) Persuade political decision-makers in a post-Snowden era to act to guide good policies, programs, and standards along the lines of the LangSec and dispersed PKI recommendations of this paper.
   This must be the first and most important step. In recent years, militaries have shied away from taking this step, as they were aware of the multitude of political problems that it would entail for them. Politicians will ask why the military made poor decisions in favor of insecure IT, and why they did not do a proper job to protect their infrastructure. Moreover, politicians will not allocate new money, so militaries may have to solve expensive IT-security problems by getting rid of tank battalions. Neither is it very popular, given the current political and economic climate in security, so militaries tended to pretend that all was fine, while trying to change slowly and 'under the radar' with only small and careful demands for increases in their IT-security budgets. Militaries have been frequently thankful for convenient and convincing lies from the IT-security industry. But politicians need to know that their high-tech, network-centric, all-sharing military apparatus is simply not operational, as soon as their adversaries are no longer goatherds with Kalashnikovs, but a determined high-tech military with a functioning secret service.
2) Acquire and keep an appropriate workforce and R&D-capabilities able to evaluate, monitor, implement, and defend critical infrastructures using a LangSec approach and PKI.
   Experience has shown that this demand is far from trivial. Militaries with a lot of moving personnel, low pay, and few incentives for a high-end professional IT-security workforce tend to fail to get the personnel they need. Bad security personnel make bad security choices and do not understand risks, demands, and options.
3) Identify and formulate high security IT demands, notwithstanding market pressures, legacies or conventional wisdom.
4) Incentivize a high security IT market through military R&D contracts and acquisition specifications.
5) Punish producers of inadequate products and markets with liability fines, business license suspensions, and penalties for downstream losses and by favoring high security products in acquisition cycles.
6) Use modernization cycles in militaries and the economy to move away from insecure solutions and onto high security IT.

In conclusion, we have argued that small building blocks and high security IT are feasible and ever more necessary paradigms for secure information societies. These concepts can secure our IT-environments to a degree far above current standards. Much of it can be composed using communication protocols automatically derived from

formal grammar, and can be authenticated using decentralized public key infrastructures.

The underlying issue of a bad market without alternatives or product liability can be mitigated by nation states and militaries acquiring new IT systems, with properties like the ones described here as required elements of new projects' specification. Only then will the incentive to build secure, defendable, and recoverable building blocks outweigh the economic benefits of making more of the same un-defendable IT systems that we continue to spectacularly fail to protect today, but that we all still depend on.

References

[1] Chemuturi, M., 2010. Mastering Software Quality Assurance: Best Practices, Tools and Technique for Software Developers. Fort Lauderdale: J. Ross Publishing, p. 9.
[2] Veracode, 2011. State of Software Security Report: The Intractable Problem of Insecure Software. [pdf] Burlington, MA: Veracode. Available at: <https://media.blackhat.com/bh-eu-12/Wysopal/bh-eu-12-Wysopal-State_of_Software_Security-WP.pdf> [Accessed 5 November 2013].
[3] Bratus, S., Locasto, M.E., Patterson, M. L., Sassaman, L., and Shubina, A., 2011. Exploit Programming: From Buffer Overflows to 'Weird Machines' and Theory of Computation. [pdf] Available at: <http://www.cs.dartmouth.edu/~sergey/langsec/papers/Bratus.pdf> [Accessed 5 November 2013].
[4] Miller, M. (Skape), 2004. Metasploit's Meterpreter. [pdf] Available at: <http://dev.metasploit.com/documents/meterpreter.pdf> [Accessed 5 November 2013].
[5] US National Vulnerability Database. Available at: <https://nvd.nist.gov/> [Accessed 5 November 2013].
[6] It is instantaneous for attacks on individual computer users at home.
[7] Gaycken, S., and Austin, G., (in press). Make Highly Secure Computing the Dominant Paradigm for International Cybersecurity. EastWest Institute Policy Papers.
[8] US Department of Defense, 1985. Department of Defense Trusted Computer System Evaluation Criteria. Available at: <http://csrc.nist.gov/publications/history/dod85.pdf> [Accessed 5 November 2013].
[9] Lost In Space, 1965. [Film] Directed by Irwin Allen. USA: Fox Television Studios.
[10] LANGSEC: Language-theoretic Security 'The View from the Tower of Babel.' [online] Available at: <http://www.langsec.org> [Accessed 13 November 2013].
[11] Wikipedia contributors. 'Chomsky Hierarchy.' Wikipedia, The Free Encyclopedia. [online] Available at: <https://en.wikipedia.org/wiki/Chomsky_hierarchy> [Accessed 5 November 2013].
[12] Lindner, F., 2010. Preventing Adobe Flash Exploitation. [pdf] Recurity Labs GmbH. Available at: <http://recurity-labs.com/content/pub/Recurity_Labs_Whitepaper_Blitzableiter.pdf> [Accessed 5 November 2013].
[13] Wikipedia contributors. 'DigiNotar.' Wikipedia, The Free Encyclopedia. [online] Available at: <https://en.wikipedia.org/wiki/Diginotar> [Accessed 5 November 2013].
[14] American National Standards Institute, 2006. ISO 20828:2006. [online] Available at: <http://webstore.ansi.org/RecordDetail.aspx?sku=ISO+20828%3a2006> [Accessed 5 November 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-65

Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities Across NATO

MATTHEW W. HOLT
Intellium LTD

Abstract. The North Atlantic Treaty Organization (NATO) has a key role to play in improving member states' and partners' overall cyber defense posture. To achieve this objective, NATO must ensure it is not imposing overlapping or conflicting requirements that may make national cyber security programs less effective, and must drive efforts to improve national incident response and international coordination. Developing these capabilities will require coordinated planning, implementation, and performance management of mature national cyber security strategies across NATO countries. Understanding all layers of the NATO cyber ecosystem, including the stakeholders' priorities, maturity levels of current guidance on cyber security, and NATO's own ability to influence and add value to each layer of its ecosystem is essential to ensure NATO can issue effective guidance.

Keywords. Cyber security posture, cyber security standards and requirements cyberspace, European Union, information communications technology, national incident response, national cyber security strategy, NATO.

Introduction

NATO's core mission is to 'safeguard the freedom and security of its members through political and military means.'[1] Due to the rapid expansion of technology over the last twenty years, cyberspace is now considered the fifth military domain (in addition to the traditional domains of land, sea, air, and space), and NATO must act accordingly to ensure Allies are able to improve their cyber security posture and manage cyber crises when they occur.

However, neither NATO Headquarters nor any individual Ally can accomplish this objective alone. NATO member states and partners must take the first step in improving their own national cyber security capabilities by outlining a National Cyber Security Strategy that addresses a minimum set of core elements. In addition to addressing national priorities, the Allies must also link their strategies to a higher-level international vision, such as the one exemplified in the NATO Policy on Cyber Defense.

At the same time, NATO and other international bodies must ensure they are not imposing overlapping or conflicting requirements that may make national cyber security programs less effective. To issue effective guidance, NATO leadership must

first understand all layers of its cyber ecosystem, including (at each level) the priorities of stakeholders, the maturity levels of current guidance on cyber security, and its own level of influence and ability to add value to relevant countries. In particular, national and international incident response represents one of the high impact areas where NATO leadership, member states and partners should work together to meet common objectives. Developing this capability should be a priority across NATO.

1. National Cyber Security Strategies

To improve their national security posture and promote the development of digital economies in the face of an increasingly complex and rapidly developing threat landscape, many NATO member states and partners are increasingly promoting a variety of national cyber security initiatives. Countries regarded as already having 'best practices' in the cyber security industry continue to improve and adapt their strategies to meet new threats. Others are creating a national agency with cyber security responsibilities and outlining the first cornerstones of a national approach.

Regardless of the current state of maturity, every country should be concentrating on developing or improving its own national cyber security strategy to address a common set of core elements.

For example, in the Netherlands (pop. 16.7 million), the Ministry of Security and Justice released *The National Cyber Security Strategy (NCSS)*[2] in June 2011 to outline national policy principles and objectives for cyber security, as well as a number of prioritized action items. Specifically, NCSS aims to:

- Set up a National Cyber Security Council and National Cyber Security Centre;
- Set up threat and risk analyses;
- Increase the resilience of critical infrastructure;
- Increase capacity for responding to ICT disruptions and cyber attacks;
- Intensify the investigation of cybercrime and the prosecution of its perpetrators; and
- Encourage research and education.

Unifying all of these activities under a single strategy and program reinforces the primary goal of improving cyber security and giving individuals, businesses, and public entities more confidence in the use of ICT, and thereby stimulating the digital economy.

Similarly, the UK (pop. 62.8 million) released *The UK Cyber Security Strategy* in November 2011, designed to 'protect and promote the UK in a digital world.' The latest revision of this strategy outlined four main objectives to improve the UK's national cyber security posture, as outlined in Figure 1.[3]

Figure 1: Objectives of the UK Cyber Security Strategy

1.1. Elements of Mature National Cyber Security Strategies

A broad review of these and other national cyber security strategies reveals that, despite their wide ranges in population, government, and culture, countries are trying to address a similar cyber threat scenario. We can thus identify a common set of elements that all mature national cyber security strategies should address:

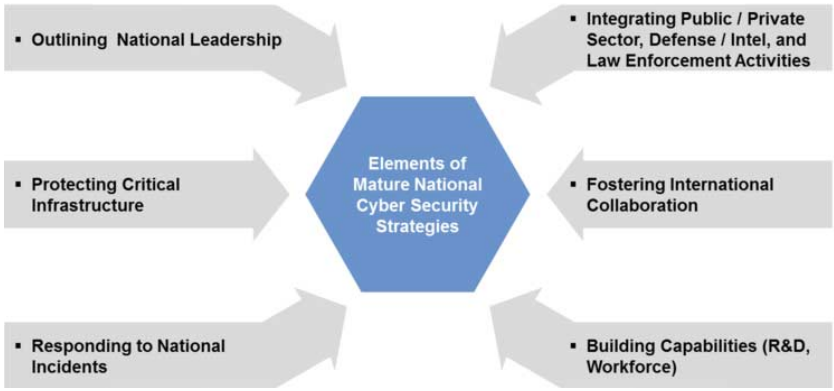


Figure 2: Elements of Mature National Cyber Security Strategies

1.1.1. Outlining National Leadership

A mature national cyber security strategy should outline the national leadership's objectives for increasing national security and the areas of activity required to achieve them. One of the objectives should be to foster the growth of the national digital economy. The strategy should clearly outline which entity will be responsible for leading the overall national cyber security program (often the entity that issues the strategy document), and include more detailed guidance on specific initiatives. There should also be clear links between the national cyber security strategy and other

national security and emergency management programs, as well as any international requirements stemming from organizations such as NATO or the European Union (EU), where applicable. In countries with highly privatized economies, the strategy should also outline approaches for engaging private sector actors through either cooperative or mandate-based models.

1.1.2. Protecting Critical Infrastructure

National leadership should identify sectors containing critical infrastructure, such as energy, telecommunications, and financial services, and outline programs to lower the risks to these critical services to acceptable levels. In free market environments, this often begins by formalizing cooperative public-private partnerships vital to the success of securing critical infrastructure. In addition to direct funding of governmental programs, governments can also provide other incentives to the private sector for establishing Critical Infrastructure Protection programs, such as preferred vendor status or limited liability in case of service interruptions.

1.1.3. Responding to National Incidents

National Incident Response activities should be organized in a process-based approach that addresses preparation, prevention, detection, analysis, response, and recovery activities. In the event of a national crisis, it should be clear which agency would be responsible for coordinating the response between relevant private and public sector stakeholders. In addition, strong Shared Situational Awareness, resulting from trusted information sharing between national and international stakeholders, should support such incident response activities.

1.1.4. Integrating Public and Private Sector, Defense, Intel, and Law Enforcement Activities

Strategic agendas and operational activities should be aligned to eliminate possible divergent measures and ensure that all stakeholders are moving towards a common national goal without overlap or gaps between major cyber security programs. While this does not imply that control of such programs should be centralized, a minimum level of visibility and interaction between stakeholders will help ensure that limited national resources are spent wisely and the capabilities of one stakeholder can be leveraged by another.

1.1.5. Fostering International Collaboration

Given the borderless nature of cyberspace, international collaboration activities should focus on building working relationships on policy and operational levels between stakeholders in different countries. Programs should be progressive in nature and formalize international relationships through multilateral agreements and organizations that can facilitate efforts in risk management, information sharing, incident response coordination, and research and innovation. In addition, national strategies must be aligned with higher level guidance issued by international bodies to which the country in question adheres (e.g. NATO, EU).

1.1.6. Building Capabilities (R&D, Workforce)

Government, NGOs, academia, and the private sector should work together to foster R&D with special attention to establishing national bodies as reference points for furthering research and innovation, and reducing dependency on other countries for cyber security solutions. At the same time, multiple agencies should be driving national awareness and capability building efforts for both the general public and enterprises around topics such as privacy, data protection, theft avoidance, etc. Tailored education and training programs for cyber security should incorporate the specialized skills and capabilities needed to build a national workforce. These programs should also identify incentives to lure the brightest minds into this field (e.g., talent competition and challenges, scholarships, project funding, etc.).

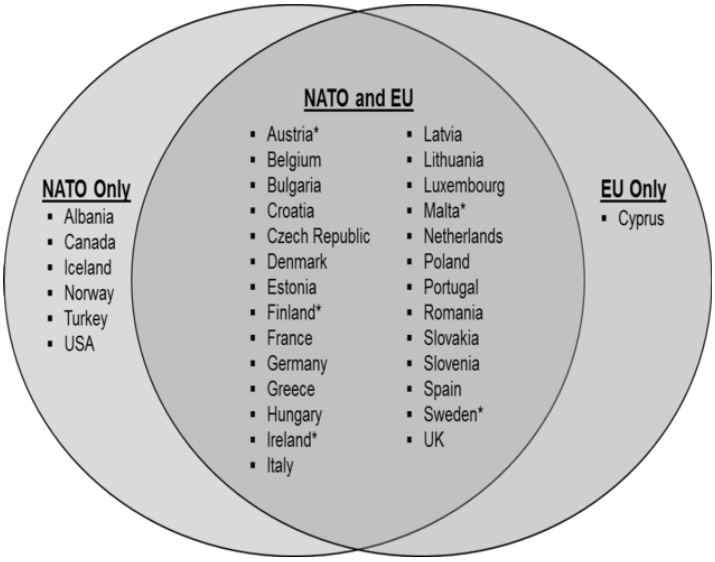
These national cyber security strategy elements should be addressed through a lifecycle approach to cyber security. This approach should focus on planning, implementing, and managing the performance of security measures and stakeholders, while also building the internal and external enablers needed to ensure the entire system functions with maximum efficiency and effectiveness.

2. International Context of National Cyber Security Strategies

In addition to the common challenges faced by any country trying to develop a national cyber security strategy, NATO member states and partners are often confronted with overlapping and potentially conflicting requirements derived from their bilateral or multilateral accords. These countries must ensure that any national strategy or legislation produced is aligned to, and is not in conflict with, the requirements of such multinational accords.

For example, Italy passed a key piece of its national cyber security legislation on January 24, 2013, which outlined the roles and responsibilities for national leadership on cyber security and reaffirmed the importance of close collaboration with EU and NATO member states. In addition to describing the organizational structure responsible for national security in terms of information-based critical infrastructures, the legislation specifically pointed out that national policy makers and practitioners in Italy must participate fully in the various fora of international cooperation, both bilaterally and multilaterally, including both the EU and NATO.[4]

This is particularly important since 22 NATO member countries and five NATO partners from the Euro-Atlantic Partnership Council (EAPC) are also EU member states, and therefore must balance their own national cyber security priorities with developing programs in NATO and the EU, amongst others.



* NATO Partner Country through EAPC
Figure 3: Overlap of NATO and EU Membership

Understanding the similarities and differences between NATO and EU cyber security strategies is critical for policy makers—not only at the national level, but also within NATO and the EU. Lack of this understanding is often the root cause of conflicting policies and objectives. For example, both NATO and EU strategies aim to improve overall security posture by improving the capabilities of each individual member state. However, the NATO Policy on Cyber Defense and supporting Action Plan focus primarily on protecting the assets of NATO headquarters and operating agencies, while the EU Strategy on Cyber Security and supporting Directive focus primarily on establishing requirements for individual member states to improve their own national cyber security postures.

2.1. NATO Policy on Cyber Defense

In June 2011, NATO adopted a new cyber defense policy that set out a clear vision of how the Alliance plans to bolster its cyber efforts. The primary focus of the NATO Policy on Cyber Defense and its supporting Action Plan is the protection of NATO's own communication and information systems. The policy also addresses cyber defense requirements for national networks that NATO relies upon to carry out its primary mission of collective defense and crisis management.

Specifically, the NATO Policy on Cyber Defense aims to:[5]

- Integrate cyber defense considerations into NATO structures and planning processes in order to perform NATO's core tasks of collective defense and crisis management.
- Focus on prevention, resilience, and defense of cyber assets critical to NATO and Allies.
- Develop robust cyber defense capabilities and centralize protection of NATO's own networks.
- Develop minimum requirements for the cyber defense of national networks critical to NATO's core tasks.

- Provide assistance to Allies to achieve a minimum level of cyber defense and reduce vulnerabilities of national critical infrastructures.
- Engage with partners, international organizations, the private sector, and academia.

2.2. EU Strategy on Cyber Security

In February 2013, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative) issued a new cyber security strategy that outlines the EU's vision in this domain, clarifies roles and responsibilities, and sets out the actions required for strong and effective protection and promotion of the EU's online environment.[6]

The EU vision presented in this strategy is articulated in five strategic priorities:

- Achieving cyber resilience;
- Drastically reducing cyber crime;
- Developing cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP);
- Developing the industrial and technological resources for cyber security; and
- Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

In conjunction with the new strategy, the Commission also issued a Proposal for a Directive of the European Parliament and the Council concerning 'measures to ensure a high common level of Network and Information Security across the Union', commonly referred to as the NIS Directive.[7] If approved, this new Directive will legally bind member states to be compliant with the defined measures for ensuring a high common level of network and information security within the EU.

2.3. Potential Overlaps / Conflicts Between National and International Strategies

The need to satisfy national and international requirements can easily create conflicting priorities for policy developers on all levels—for example, based on differences in policies on data privacy and incident response. In addition, countries are using information security standards to meet different objectives and, in some cases, competing and contradictory standards are being imposed.

2.3.1. Data Privacy

For example, some elements of the new EU strategy and accompanying Directive proposal are already coming under heavy criticism due to potential conflicts with other EU and national legislation on related data protection topics. In July 2013, the European Data Protection Supervisor (EDPS), an independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection, issued a 26-page document outlining its concerns regarding the new EU strategy and 'how these principles will be applied in practice to reinforce the security of individuals, industry, governments, and other organizations.'[8]

EDPS argues that the EU strategy does not clearly define how EU Agencies with responsibilities in cyber security (e.g. ENISA, Europol) will interact with national Data Protection Authorities, and that it fails to take due account of the role of data protection

law and current EU proposals in promoting cyber security—for example, the proposed Data Protection Regulation and the eTrust Regulation.

This lack of clarity can create difficulties for national policy makers when outlining the roles and responsibilities of national leadership in their own cyber security strategies, and will likely lead to varying interpretations of EU policies by different countries.

EDPS further points out that:

> While measures to ensure cyber security may require the analysis of some personal information of individuals, for instance IP addresses that can be traced back to specific individuals, cyber security can play a fundamental role in ensuring the protection of privacy and data protection rights in the online environment, provided the processing of this data is proportionate, necessary, and lawful.[9]

The fact that this type of criticism is emerging from within EU bodies themselves further confirms the difficulties in issuing an international strategy that does not overlap with other efforts or infringe on national legislation.

2.3.2. International Incident Response

Similar to contradictions in data protection regulation, rules are not clearly defined even with respect to joint response to a cyber crisis in a NATO country that is also an EU member state. This can easily create difficulties for national incident response practitioners looking to define the international dimensions of their programs.

For example, the NATO Strategic Concept states that the Alliance will 'defend against any threat to the safety and security of its populations,'[10] including emerging security challenges such as cyber threats. In this sense, NATO asserts that it will provide coordinated assistance to an Ally in the midst of a cyber crisis. Specifically, the NATO Policy on Cyber Defense reiterates that any collective response will be subject to the political decisions of the North Atlantic Council, and that NATO will maintain strategic ambiguity as well as flexibility on how to respond to different types of crises that include a cyber component.

Although NATO aims to enhance consultation mechanisms, early warning, situational awareness, and information sharing among the Allies, there are intentionally no formal international incident response plans that outline exact roles and responsibilities of NATO leadership or member states and partners in the case of a joint response to a major cyber crisis. To facilitate these activities, however, NATO has implemented a framework of cyber defense—a Memoranda of Understanding (MOU)—between Allies' national cyber defense authorities and the NATO Cyber Defense Management Board. While the MOU provides a strategic forum for discussion and formation of long-term strategic plans, there are serious questions about how effective these strategies would be against a real-time, large-scale cyber crisis that can take an entire national critical infrastructure out of service in a matter of seconds.

At the same time, the EU strategy points out that a particularly serious cyber incident could constitute sufficient ground for a member state to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union). However, this strategy does not provide any insight or guidance as to what qualifies as 'serious' or what type of support to expect (or from whom) in the event of invocation of Article 222. Again, one could question whether or not this type of policy-based approach is adequate to deal with the speed and potential impact of a cyber-based crisis.

As a result, when outlining the incident response components of national strategies and legislations, in particular regarding international collaboration, NATO member states and partners are not receiving enough clear and consistent guidance. Therefore, in the interest of their own national security, they often operate either alone or through other bilateral or multilateral agreements that can overlap or conflict with one another, and will likely require retro-fitting to NATO, EU, or other programs in the future.

3. How NATO Can Help

3.1. How NATO Guidance Can Add Value

Within the NATO cyber security environment, individual stakeholders in member states and partners interact through a complex system that consists of four distinct layers. To pragmatically add value to this ecosystem, NATO must understand the priorities of stakeholders, the maturity levels of current guidance, and its influence and ability to add value at each level.

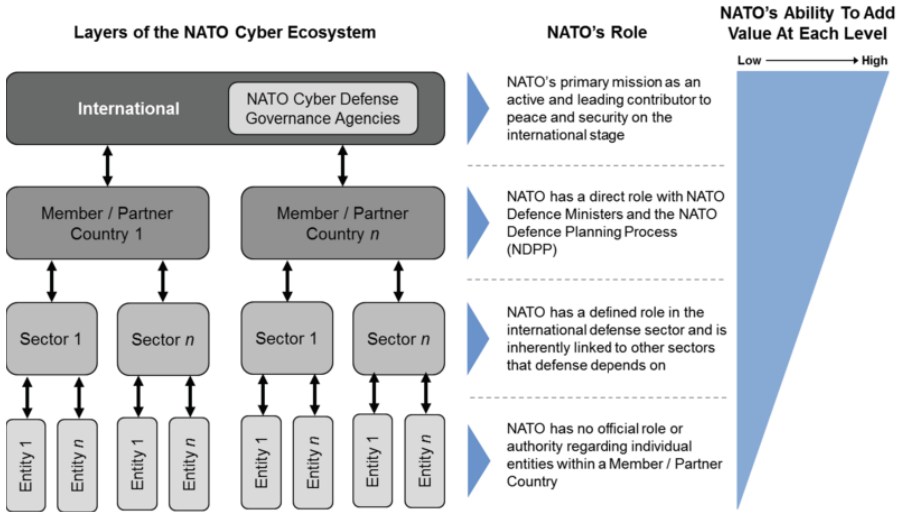


Figure 4: Layers of the NATO Cyber Ecosystem

At present, there is a great deal of guidance available regarding cyber security at the entity level. Organizations such as the National Institute of Standards and Technology (NIST) in the US, the International Organization for Standardization (ISO), the SANS Institute, and many others have spent decades developing and fine tuning cyber security guidelines that have been implemented by thousands of individual entities worldwide. Given this level of maturity and the fact that NATO has no authority to set standards for individual entities in member and partner countries, NATO should not invest a great deal of resources in trying to develop and disseminate new guidance on this level.

However, as we move up through the levels, the maturity of available cyber security guidance diminishes, while NATO's role and ability to influence stakeholders increases. For example, the availability of sector-level guidance is significantly lower than at the entity-level. Although there are a handful of sector-specific cyber security standards issued by organizations such as the North American Electric Reliability

Corporation (NERC) (e.g. Standards CIP-002-1 through CIP-009-1) and the International Telecommunication Union (ITU) (e.g. Standards X.1051 and E.408), there are few internationally recognized sector-specific 'best practices' that have been implemented worldwide.

NATO does not have the authority to impose cyber security requirements and standards directly on individual defense sector stakeholders in member and partner countries. It does, however, have the ability and purchasing power to influence the industry to deliver higher assurance products and services and better address cyber security within the defense sector overall. For example, by communicating standards and requirements to defense contractors and suppliers through the NATO Industrial Advisory Group (NIAG), then creating initial demand for these products and services, NATO can encourage stakeholders to develop effective solutions that support the defense sector capabilities member states and partners need to meet NATO cyber security objectives and requirements.

At the national level, NATO's influence can be significant. Even though NATO does not have the authority to force member states and partners to take any specific action, it can provide guidance for national leadership on how to reduce risks in sectors that support defense and NATO objectives. For example, NATO can start by identifying (or providing guidance on how to identify) the interdependencies between the services it provides to the Allies and the critical national networks used to support these services.

However, NATO is positioned to have the strongest influence at the international level. There is currently no recognized best practice outlining how individual countries should interact with each other on key elements of international collaboration, such as developing common minimum security standards, responding to multinational or cross-border cyber incidents, or identifying mutually critical infrastructure. In these areas, NATO is authorized to (and should) identify minimum standards that member states and partners should meet before being able to collaborate with one another through NATO's own network infrastructure. NATO can also invest its own funds to increase the security of this international network.

Regardless of the level targeted, any guidance issued by NATO would only be effective if implemented by a significant number of member and partner countries. Since NATO does not have the authority to force any individual country, sector or entity to take specific actions, policy makers must find other ways to encourage stakeholders to adopt such guidance and standards. NATO representatives should therefore engage stakeholders across all ecosystem layers early and continuously to both ensure that all perspectives are considered, and facilitate buy-in of the final products.

Additionally, if NATO does not monitor the implementation of its guidance and appropriately measure outcomes, there will be no means to judge its effectiveness. In this regard, NATO should first assess the current cyber security capability levels of member and partner countries prior to initiating the development of specific guidance. In addition to establishing a baseline against which progress can be measured, this will help NATO identify the specific areas where capabilities are less mature, and therefore where guidance from NATO can add the most value. Further, building consensus on new requirements would become easier if NATO were able to clearly demonstrate and measure improvements made in the past.

Such a program should also provide feedback to member states and partners in the form of a sanitized benchmark tool that would allow each stakeholder to anonymously

compare themselves to others. In areas where a specific stakeholder is significantly below average, NATO could then provide even more specific guidance to bring them up to an acceptable level. Involving NCIRC and CIS Operating Authorities in this type of activity would also help strengthen the community by promoting a group-level approach to cyber security, rather than focusing on individual entities.

4. Prioritizing Incident Response across NATO

While all elements of a mature national cyber security strategy are equally important for its successful implementation, cyber security activities at the national and international level often begin with pragmatic coordination of individual entities within a specific country or sector in the area of National and International Incident Response (NIIR). This priority is often driven by the realization that the country or sector in question is vulnerable to large-scale cyber crisis, in some cases already suffered in neighboring countries.

While it may take some time, even years, for some countries to make the necessary improvements to their critical infrastructure to prevent such incidents, national leaders tend to focus on immediate answers to what the country would do if they were to suffer a cyber crisis today. As a result, there is a stronger focus on developing incident response capabilities as the starting point for longer-term programs, such as Critical Infrastructure Protection. Given that crisis management is one of NATO's core tasks, the Alliance should also invest in improving incident response for its own networks and reducing the impacts of incidents on member states.

NIIR, therefore, represents one of the key, high-impact areas where NATO leadership, member states and partners should work together to achieve common objectives.

Since there is currently no globally recognized single set of best practices or standards to manage cyber incidents in an efficient and effective manner at the international level, NATO can play a critical role in guiding Allies to establish a basic framework of NIIR core aspects and encourage them to embed these requirements in their own national cyber security strategies.

For example, an effective NIIR program must be founded on at least two basic principles. First, all relevant stakeholders must be aware of the cyber activity happening inside and around their own organizations, as well as how this may impact other stakeholders at the national and international level. Second, agencies tasked with managing cyber crises must have the authority to take the required actions or instruct others to do so when needed.

4.1. Shared Situational Awareness (SSA)

One of the first priorities in establishing a NIIR program across NATO must be building the capability to recognize if and when incidents are actually taking place and finding ways to limit their impact on the entity under attack as well as on other related entities at the sector, national, or international level. This should occur through Shared Situational Awareness (SSA) between stakeholders that have previously built trusted information sharing capabilities.

SSA is based on a common level of awareness that individual entities in a group possess about the status of events that affect the entire group. Ideally, every entity

would be equally aware of what is happening in its vicinity. With a broader view of common threats, each entity would be able to prevent and respond to incidents more efficiently and effectively.

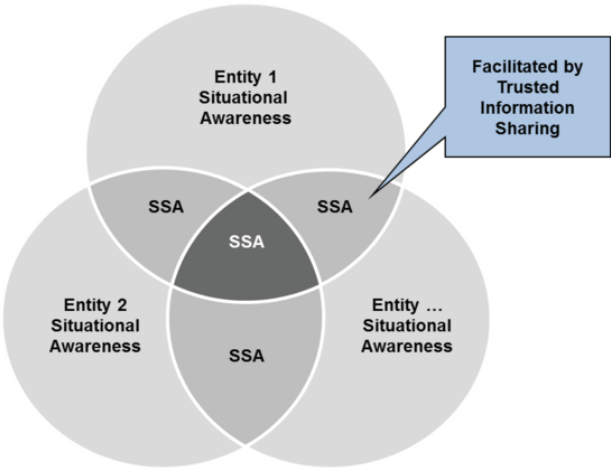


Figure 5: Shared Situational Awareness

Ensuring all stakeholders are able to share valuable information on serious incidents requires *inter alia* a series of clearly defined requirements regarding what type of information should be shared, who will have access to it, and what security measures should be taken to protect the information once released by its original owner. The complexity of this sensitive exchange of information grows proportionately with the size of the group, and perhaps exponentially when the members of the group are sovereign states with individual national security requirements.

Many individual countries have developed strong national Information Sharing programs that could be leveraged as good practices for an international model. These programs tend to focus on aligning similar stakeholders into groups, then aligning the groups into a national program. The US[11] and UK[12] have been particularly successful in this area:

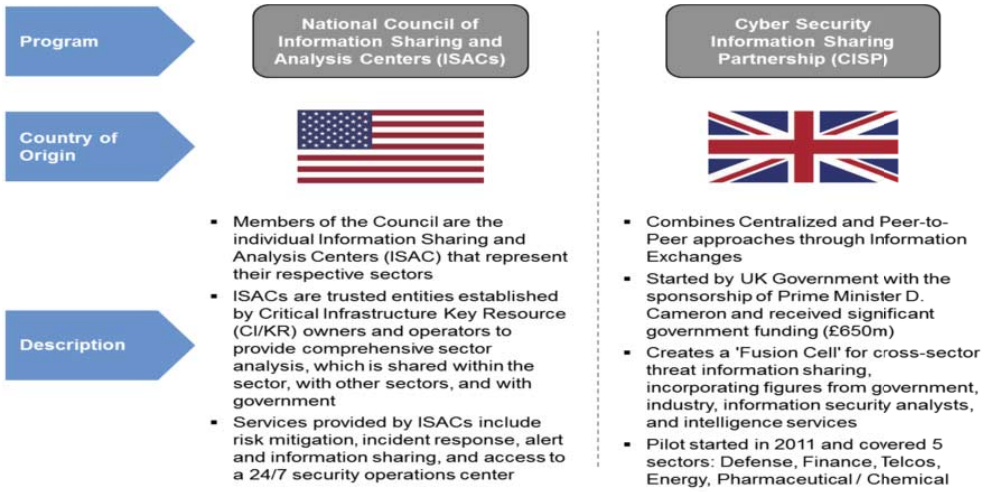


Figure 6: US and UK Information Sharing Programs

However, possessing this capability 'inside the wall' is not enough. This holds true whether the 'wall' is protecting a single entity, a sector, or a country. A single-nation approach is not adequate to protect against mature adversaries, often either located in or sponsored by foreign states. Since the cyber security threat landscape is international in nature, and attacks often come from outside national boundaries and jurisdictions, practitioners developing NIIR strategies need to place particular emphasis on international dimensions. Failure to do so at the planning stages will lead to costly and potentially unfeasible retro-fitting into an international approach developed further down the road as they begin participating in multinational exercises or enter bilateral agreements with other countries. Even then, each new bilateral agreement can present conflicting requirements with those previously implemented.

By providing guidance on how member states and partners can facilitate SSA across all four layers of its cyber ecosystem, NATO can help ensure individual stakeholders are aware not only of what is happening within their own boundaries, but also with other stakeholders on a sector, national, or international scale, as appropriate. This pooling of resources and capabilities helps each stakeholder improve its own security posture, while also improving the group's security posture overall.

In particular, NATO should focus on developing guidance to help member states and partners answer key questions such as:

- Why are SSA and NIIR elements of national strategies important to help NATO realize its cyber defense objectives?
- What type of information should NATO stakeholders be sharing at the entity, sector, national, and international levels?
- What protocols should member states and partners follow to participate in the collection, analysis, and dissemination of information on a trusted basis within the NATO ecosystem?
- What technical requirements must member states and partners systems meet before being allowed to connect to NATO information sharing platforms?
- How can practitioners in member states and partners raise awareness on this topic to ensure they receive leadership support for program implementation?

For example, the NATO Computer Incident Response Capability (NATO NCIRC) and the Belgian Defense CERT have worked together to develop the Malware Information Sharing Platform to exchange information about targeted malware and attacks within a group of trusted partners.[13] It is worth noting that the EU has also funded significant research in this area to facilitate the development of trusted international information sharing platforms such as the Critical Infrastructure Warning Information Network (CIWIN)[14] and the National & European Information Sharing & Alerting System (NEISAS).[15] Continued research and development of these types of models and tools is needed to ensure the widest possible uptake in the international community.

Another focus area could include activities such as formalizing a NATO sub-group within an existing international CERT community. For example, participants in the Forum of Incident Response and Security Teams (FIRST) are part of a network of computer security incident response and security teams that work together voluntarily to deal with computer security problems and their prevention. Many of the 281 teams across 61 countries currently participating in FIRST activities are located in NATO member and partner countries, implying that a certain level of capability already exists.

To improve on this, NATO can offer specific guidance for other teams such as national or defense CERTs of member states and partners to join groups such as these. This could come in the form of assessment and advisory services through NCIRC to help other CERTs understand the necessary steps to improve capabilities to the level needed to join groups such as FIRST. Doing so would also help the NATO sub-group connect to other organizations outside NATO, further increasing the range and value of information available.

To measure and demonstrate the value and impact of these types of activities, NATO should leverage its ongoing cyber defense exercise programs, such as Cyber Coalition[16] and Locked Shields,[17] to compare incident response capabilities year-on-year and determine if the guidance issued has actually improved the capabilities of stakeholders.

4.2. Legal Mandates

When assigning roles and responsibilities within a NIIR program, national leaders must also be sure to issue the mandates and authorities needed to enable appropriate agencies (e.g. national CERTs, public sector entities, ISPs, defense, intelligence, law enforcement) to take the required action or instruct others to do so.

For example, implementing a NIIR plan in most countries will require one or more lead agencies to coordinate activities across a wide range of stakeholders. It is critical for the lead agency to have the means available to influence the activities of these stakeholders. This can be particularly complex when a new agency is overseeing previously siloed activities across multiple actors that have reached a high level of individual maturity. Simply assigning a lead role to an agency will not be effective if that agency does not have the legal authority and instruments needed to implement its mandate.

In addition, other NIR stakeholders must also have the authority to execute the roles they have been assigned by national leadership within the context of the NIR plan. For example, recent legislation in the Netherlands commonly referred to as the 'Net Neutrality Law' (May 2012)[18] clarifies what ISPs can and cannot do in terms of influencing the traffic they manage, taking users offline, and examining message content—these are all key elements of an effective response to cyber security incidents. While generally restricting the conditions under which an ISP can interfere with user traffic, specific conditions surrounding security-related incidents are given as exceptions. For example, Article 7.4.a.2 states that:

> If an infraction on the integrity or security of the network or the service or the terminal of an end user […] is being caused by traffic coming from the terminal of an another end user, the provider, prior to the taking of the measure which hinders or slows down the traffic, notifies the end user in question, in order to allow the end user to terminate the infraction. Where this, as a result of the required urgency, is not possible prior to the taking of the measure, the provider provides a notification of the measure as soon as possible.[19]

This clause clearly gives an ISP the authority needed to take action to respond to threats such as botnets, spam, DDOS attacks, and other activity originating from its connected user base. Other clauses in the law authorize ISPs to take other actions

necessary to ensure the integrity and security of the networks and services to include, within defined limits, wiretapping (Article 11.2.a.2.b) and disconnecting users (Article 7.6.a).

Other examples of NIR-related activities that might require legal authorization include activation of an Internet 'Kill Switch', reading e-mail content, tracing sources or destinations of communications, access to or disclosure of stored communications, and sharing subscriber information and transactional records.

Given the current international debate surrounding the balance between privacy and security, national leaders must provide clear guidance and authorization to stakeholders on how to manage these issues before an incident occurs. Failure to do so could lead to decreased efficiency of response activities during an incident, as well as complex legal and political conditions after action has been taken (or not taken).

Recommendations and Conclusions

The following recommendations are intended to guide NATO and its member states and partners to develop efficient and effective national cyber security strategies, issue coherent standards and requirements, and improve national and international incident response capabilities:

- **Recommendation 1:** Each NATO member and partner country should develop a national cyber security strategy that outlines core elements of national leadership, protecting critical infrastructure, responding to national incidents, integrating stakeholder activities, fostering international collaboration, and building internal capabilities.
- **Recommendation 2:** National policy makers should align their national cyber security strategies to higher-level guidance, such as NATO and EU requirements. At the same time, international policy makers should coordinate their efforts to ensure they are not issuing requirements to countries that create conflict or make the country less effective at cyber security.
- **Recommendation 3:** NATO should focus on understanding how it can add value to each layer of its cyber ecosystem and prioritize its efforts where they can have the greatest measureable impact on NATO's core tasks of collective defense and crisis management.
- **Recommendation 4:** All NATO stakeholders should work together to prioritize the development of NIIR capabilities, focusing in particular on SSA between the Allies and leveraging NCIRC to build knowledge, capabilities, and relationships.

Given the number and digital economic maturity of its constituents, as well as the capabilities of its existing cyber security governance structure, the NATO ecosystem represents one of the best opportunities for a large group of countries to improve their individual and collective cyber security posture through coordinated planning, implementation, and performance management of national cyber security strategies.

To achieve this objective, each of the Allies must first ensure that it is constantly striving to develop or improve its own national cyber security strategy which covers a common set of core elements, including linking to higher level international guidance as appropriate.

In this regard, NATO leadership must ensure any guidance issued does not overlap or create conflict with other national or international requirements applicable to member states and partners. Doing so requires a deep understanding of the stakeholder priorities, the maturity levels of current guidance, and NATO's own ability to influence and add value to each layer of its own cyber ecosystem.

In particular, few elements of a national cyber security strategy are as tangible as incident response. With security operations centers, CERTs, early warning and detection systems, etc., this represents a high-impact area where NATO leadership and member states and partners should work together to meet common objectives in a highly visible way. Developing this capability should be a priority across NATO.

References

[1] NATO Basic Points. A Political and Military Alliance. [online] Available at: <http://www.nato.int/nato-welcome/index.html> [Accessed 8 November 2013].
[2] Dutch Ministry of Security and Justice, 2011. The National Cyber Security Strategy (NCSS): Strength through cooperation. [online] Available at: <https://www.ncsc.nl/english/current-topics/news/national-cyber-security-strategy-launched.html> [Accessed 8 November 2013].
[3] UK Cabinet Office, 2011. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. [online] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> [Accessed 8 November 2013].
[4] Office of the Prime Minister of Italy, 2013. Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013: Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale. Rome. Rome: Office of the Prime Minister of Italy.
[5] NATO Public Diplomacy Division, 2011. Defending the networks: The NATO Policy on Cyber Defense. Brussels: NATO.
[6] European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final). Brussels: European Commission.
[7] European Commission, 2013. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: concerning measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final). Brussels: European Commission.
[8] European Data Protection Supervisor, 2013. Credible Cyber Security Strategy in the EU Needs to be Built on Privacy and Trust. [press release] 17 June 2013. Available at: <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2013/EDPS-2013-06_Cyber%20Security_EN.pdf> [Accessed 8 November 2013].
[9] Ibid.
[10] NATO Summit, 2010. 2010 Strategic Concept: Active Engagement, Modern Defense. Lisbon: NATO.
[11] National Council of ISACs (NCI). Available at: <http://www.isaccouncil.org/home.html> [Accessed 8 November 2013].
[12] UK Cabinet Office, 2013. Government Launches Information Sharing Partnership on Cyber Security. [press release] 27 March 2013. Available at: <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> [Accessed 8 November 2013].
[13] Vandeplas, C., 2013. Malware Information Sharing Platform. [blog] 10 March. Available at: <http://christophe.vandeplas.com/2013/03/misp-malware-information-sharing.html> [Accessed 8 November 2013].
[14] Critical Infrastructure Warning Information Network (CIWIN). [online] Available at: <https://ciwin.europa.eu/Pages/Home.aspx> [Accessed 8 November 2013].
[15] National and European Information Sharing and Alerting System (NEISAS). [online] Available at: <http://www.neisas.eu/> [Accessed 8 November 2013].
[16] NATO, 2011. Cyber Coalition 2011 exercise tests NATO procedures for cyber defense. [online] Available at: <http://www.nato.int/cps/en/natolive/news_82213.htm> [Accessed 8 November 2013].
[17] NATO Cooperative Cyber Defense Centre of Excellence, 2013. Locked Shields (CDx). [online] Available at: <http://ccdcoe.org/401.html> [Accessed 8 November 2013].
[18] Daalen, D., 2011. Translations of Key Dutch Internet Freedom Provisions. Verdedigit Digitale Burgerrechtent [blog] 27 June. Available at: <https://www.bof.nl/2011/06/27/translations-of-key-dutch-internet-freedom-provisions/> [Accessed 8 November 2013].
[19] Ibid.

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-81

Evolution of National and Corporate CERTs - Trust, the Key Factor

OLAF KRUIDHOF
Capgemini, The Netherlands

Abstract. This paper discusses the evolution of Computer Emergency Response Teams (CERTs) due to trends in technology and society. It shows how these trends affect the selection of services a CERT can provide to its constituency, and the effects on its resources. The argument is that CERTs need to focus more and more on the specific services they can provide. The selection of these services must be driven by the objectives of their parent organization, the constituency they serve, and the urgency by which services must be provided. The paper further asserts that cyber security organizations (highly) specialized in a limited number of tasks should collaborate with others in order to effectively handle incidents. Trust among participants represents the basis for any successful collaboration. Trust, however, only exists between people. Thus, several other elements need to be in place in order to extend individual trust to organizations.

Keywords. Cyber security, computer emergency response teams, information sharing, security services, technology trends, trust building.

1. Introduction

1.1. Document Structure

After a brief definition of some publicly available terms and references, the first section discusses objectives, capabilities, and services of CERTs, types of CERTs, and their evolution. The second section discusses technology trends, including cyber security, and the third section explores their effects on CERT operations. The final section describes ways to gain the trust and respect necessary for successful collaboration between CERTs.

1.2. Terminology

According to the Carnegie Mellon University (CMU) designation, the term CERT (Computer Emergency Response Team) refers to a team of IT security experts whose main business is to respond to computer security incidents — the first team was created in 1988 in response to the Morris Worm incident. The term CERT is a registered service mark of CMU and is licensed to other teams around the world.

As an alternative, the term CSIRT (Computer Security Incident Response Team) also refers to a team of IT security experts designated to respond to computer security incidents. This term, however, is more accurate since it reflects a broader array of security services provided, beyond reactive functions.

Terms like Security Operations Center (SOC) and Network Operations Center (NOC) are also used, mostly in industry. Although their names suggest an operational responsibility, they are often tasked with similar broad duties as a corporate CERT or CSIRT.

The term CERT appears to be more commonly used for national and governmental security teams. Since this paper focuses primarily on (multi-) national or governmental CERT operations, the term CERT is used as an equivalent of CSIRT, SOC and the likes.

1.3. Public Information

Since the first cyber security incident, a significant body of work has been developed on the topic of countering computer security incidents. The Software Engineering Institute (SEI) at Carnegie Mellon University has been and continues to be an important source for literature on defining, establishing and managing CERTs.

In addition, the European Union—and the European Network and Information Security Agency (ENISA) in particular—has developed a large collection of material to guide member states in creating and running national cyber security centers, and ways to encourage collaboration between them.

In various other countries around the world, such as in the Asia Pacific and South America regions, CERTs have been established, and guidance and lessons learned from their operations have been documented.

The volume of existing literature illustrates the importance of cyber security as a topic and the scale of initiatives undertaken worldwide to handle threats and incidents.

The vast majority of CERT-related information available provides useful guidance for establishing governmental and national CERT initiatives. Clearly, trade and industry are also spending significant amounts of time and money on cyber security incident responses. However, little information is available from an industry perspective about the creation and functioning of CERTs. Most of the publicly available industry information on cyber security stems from security companies that offer commercial services and products to handle cyber threats and incidents (e.g. Symantec, Kaspersky, McAfee, etc).

For obvious reasons, virtually no information is available on the activities of operational CERTs, whether national, governmental or industrial. Some useful information on collaborations between CERTs and information sharing bodies is available through other organizations such as Information Sharing and Analysis Centers (ISACs). Considering the dynamism of the cyber security field and all available sources, this paper prioritizes the more recent information.

2. CERT Operations

A well-functioning CERT should provide a carefully selected set of services to its well-defined constituency (customers) in order to fulfill the mission of its parent organization. As shown in the past 25 years, it is not sufficient for a CERT to bring together a group of IT security experts and task them with providing certain services. A CERT needs to be a well-prepared, well-equipped, and well-managed organization. Therefore, a management structure, support structure, and clear mandate are also key capabilities that must be put in place.

ENISA identified a set of baseline capabilities for national and governmental CERTs.[1] These capabilities are categorized into four areas:

- Mandate & Strategy — the powers and justifications detailed in a strategic document on cyber security granted by the respective government to the team;
- Service portfolio — the services that a team provides to its constituencies or that it uses for its own internal functioning;
- Operational capabilities — the technical and operational requirements that a team must comply with; and
- Cooperation capabilities — requirements on information sharing with other teams. This may be partly covered by the previous three categories.

These areas are very similar to the elements in the CSIRT Framework, designed by CMU/SEI.[2]

When setting up a CERT, these four capability areas should be addressed consistently. Typically, the first step in creating a CERT is to establish its mandate and strategy and use that in the second step to derive the required service portfolio. In step three, the service portfolio should help define the necessary operational and cooperation capabilities. However, this should be a cyclical process, where the service portfolio (i.e. the results that can be delivered) influences the mandate and strategy, the operational capabilities determines the feasibility of the services delivered, and so forth.

Two types of cycles can be expected. The first iteration should take place at the incipient stages of a CERT. The capability areas should be addressed at least twice in order to ensure that they are consistent and coherent. Once a CERT is in operation for at least some time, additional iterations through the four areas should be made in order to respond coherently to trends and developments in the cyber domain, and assure that assets are being protected. This evaluation will eventually lead to an evolution of the service portfolio and required capabilities.

2.1. Mandate & Strategy

As part of the Mandate & Strategy, CERTs must have a well-defined area of operation, team objectives, audience, and specific types of assets to protect. Although cyber incidents do not respect national borders, the operations of a CERT will be bound by a legal and regulatory framework, which will include the geographical area where a CERT is allowed to operate.

Typically, the objectives for national CERTs are stated in terms of coordination and facilitation with other CERTs within state borders, and cross-domain CERTs nationally and internationally. Governmental CERTs are responsible for the protection of governmental ICT infrastructure, often including critical information infrastructure. As a result, national and governmental CERTs usually serve two types of constituencies. While national CERTs serve a broad audience ranging from the government to private organizations and civilians, the constituency of governmental CERTs consists of government staff that manages government ICT infrastructure.

The differences in objectives and constituencies should shape a CERT's strategy and evolution for answering the challenges presented by cyber adversaries.

2.2. Service Portfolio

The portfolio of services that is widely used as the de facto set of CERT services has been presented by CMU in 2002.[3] The portfolio is organized in three categories:

- Proactive Services: performed before an incident occurs or is detected.
- Reactive Services: executed when an incident becomes known.
- Security Quality Management Services: continuously executed in order to ensure incidents can be dealt with.

Table 1. The portfolio of CERT services

Proactive Services	Reactive Services	Security Quality Management Services
- Announcement - Technology Watch - Security Audits or Assessments - Configuration and Maintenance of Security Tools, Applications, and Infrastructure - Development of Security Tools - Intrusion Detection Services - Security-Related Information Dissemination	- Alerts and Warnings - Incident Handling • Incident Analysis • Incident Response on Site • Incident Response Support • Incident Response Coordination - Vulnerability Handling • Vulnerability Analysis • Vulnerability Response • Vulnerability Response Coordination - Artifact Handling • Artifact Analysis • Artifact Response - Artifact Response Coordination	- Risk Analysis - Business Continuity and Disaster Recovery Planning - Security Consulting - Awareness Building - Education / Training - Product Evaluation or Certification

In order to select the appropriate combination of services that will allow a CERT to fulfill its mission, the broad objectives stated in the mandate need to be refined. Although this process of refinement will most likely lead to different results for each individual CERT, the following baseline set of objectives that should be included in each CERT's portfolio is offered:

- Identification of security threats and potential incidents;
- Detection of security threats and incidents;
- Coordination of incident response activities;
- Containment of security incidents;
- Mitigation of security incidents;
- Attribution of security threats and incidents;
- Business Continuity despite security threats; and
- ICT resilience against security threats.

Each of the services in the portfolio serves one or more CERT objectives, and main objectives can be identified for each service. The following table presents a mapping of CERT services and corresponding main objectives which can be used to define a clear focus for selecting services to be provided by each specific CERT. The mapping does not imply that services cannot support other objectives as well. However, the aim is to provide guidance in selecting the most relevant services for any particular CERT.

Table 2. CERT Services per type of CERT

CERT Services' main focus	Identification	Detection	Coordination	Containment	Mitigation	Attribution	Business Continuity	ICT resilience	Coordinating CERT	Servicing CERT	Thematic CERT	Product CERT
Proactive Services												
Announcements	x								x	x	x	x
Technology Watch	x								x	x	x	x
Security Audits or Assessments	x	x							o	x		
Security Tools, Applications, and Infrastructures	x	x							o	x	o	o
Development of Security Tools	x	x							o	x	o	x
Security-Related Information Dissemin	x								x	x	x	x
Intrusion Detection Services		x								x		
Reactive Services												
Alerts and Warnings				x	x					x	x	x
Incident Handling												
Incident analysis				x	x	x			x	x	x	x
Incident response on site					x					x		x
Incident response support					x					x	o	x
Incident response coordination			x	x		x			x		x	
Vulnerability Handling												
Vulnerability analysis				x	x					x		x
Vulnerability response					x					x	o	x
Vulnerability response coordination			x	x	x				x		x	
Artifact Handling												
Artifact analysis				x		x			x	x		x
Artifact response				x	x					x	o	x
Artifact response coordination			x	x		x			x		x	
Security Quality Management Services												
Risk Analysis								x		x	o	
Business Continuity and Disaster Recovery Planning							x		x	x	x	
Security Consulting								x		x	o	x
Awareness Building							x		x	o	x	o
Education/Training							x		x	x	o	o
Product Evaluation or Certification								x		x	x	x

2.3. Types of CERTs

As discussed above, the Mandate & Strategy of a CERT, and especially its objectives, will define what services a CERT can provide and which constituency it can serve. This allows for the identification of different types of CERTs with different sets of services (see Appendix A – CERT Services per type of CERT).

- A **Coordinating CERT** coordinates cyber security related tasks between more specialized CERTs. In order to achieve this overall objective, a Coordinating CERT is likely to focus on Identification, Coordination, Attribution and Business Continuity. As a result, one may expect the service portfolio of a Coordinating CERT to contain at least the services in the proactive section, several of the ones in the Security Quality Management Services category, and the coordination services in the reactive section.
- A **Servicing CERT** provides proactive and reactive security incident services. A Servicing CERT focuses on handling incidents in various types of IT infrastructure (e.g. critical infrastructures like the power grid, or business infrastructures like a local computer network). A Servicing CERT can be part of an organization where all employees represent its constituency, or it can be a separate organization that provides its services on a commercial basis to one or more companies. The objectives of a Servicing CERT tend to cover the full spectrum of security objectives listed above, either as an in-house organization or as a commercial company. Therefore, a Servicing CERT can be expected to cover the full service portfolio.
- A **Thematic CERT** is a network of collaborating CERTs unified by a particular theme (e.g. ICS-CERT for oil & gas). The main focus of a Thematic CERT is a proactive exchange of information about specific threats and vulnerabilities and how to counter them, supported by theme-specific tools. Thematic CERTs can have arrangements for mutual support in case of a cyber emergency. Similar to a Coordinating CERT, a Thematic CERT is likely to focus on Identification, Coordination, Attribution and Business Continuity. Additionally, a Thematic CERT will support its members by enabling domain-specific Detection, Mitigation and ICT resilience. Achieving the extended set of objectives will require a more elaborate set of services. Other specialized organizations may choose to limit their objectives to information sharing only. Such organizations are often called Information Sharing and Analysis Centers (ISAC). Examples are the US IT-ISAC that aims at being 'the definitive source for security information impacting the IT Sector'[4] and the European FI-ISAC that shares cyber security information between parties in the financial sector.
- A **Product CERT** focuses on handling security incidents related to a certain (family of) product(s), and is normally provided by the vendor of the product. A vendor will offer security services via a Product CERT to its customers as a mean of assurance that its products will operate as expected. A Product CERT will focus on sharing information concerning threats and vulnerabilities to a specific product and mechanisms to handle incidents and artifacts. In order to fulfill the needs of its constituency, a Product CERT is likely to focus on Identification, Detection, Containment, Mitigation and ICT Resilience. A Product CERT will provide many similar services to a Servicing CERT, albeit that they will be limited to the vendor's product(s).

2.4. Evolution of a CERT - Operational and Collaboration Capabilities

Once a CERT has been established, a common pattern can be identified for the evolution of its operational capabilities. The initial drivers for establishing a CERT

reflect a sense of urgency due to, for example, the increase in the number and severity of computer security incidents, an enhanced cyber security awareness, new laws and regulations for protecting information assets or, as in the case of a Coordinating CERT, the realization that individual organizations cannot provide sufficient protection against cyber threats that affect the general public.

The first stage in creating a CERT is to provide reactive services—the ability to respond to incidents by containing and mitigating threats. Usually, the Servicing CERT of an organization provides such responses on-site. Obviously, the CERT needs to first have the right staff and tools. The tools must be based on the technology used by the constituency, while the staff needs to have the appropriate skill set to understand the technology, the infrastructure, and the tools they use. An investment in staff training is essential. In general, the initial staff will be modest, about 10 to 12 full-time equivalent (FTE). As a preparatory step, CERTs that are successful will have established their own network of trusted partners (e.g. with the Product CERT of the vendor of a key product or technology) that will provide information and support in times of crisis. The base for this type of partnerships is mutual *trust*; trust between individuals. Responding to an incident requires trustworthy partners that can gain access to the affected ICT infrastructure and are allowed to make modifications using their own tools. This requires trust in the person, his or her abilities, and the tools used. Normally, a screening process and some structures for compartmentalized information sharing are put in place in order to obtain a basic level of formalized trust, but at this stage the bottom line is still trust in people.

The second stage of successful CERTs is building (ICT) resilience against threats and limiting vulnerabilities. The CERT should extend its capabilities in order to detect and analyze vulnerabilities and threats and their potential impact on an organization's infrastructure. In addition, they should be able to ensure ICT infrastructure resilience, enabling risk analysis and product evaluation or certification. Finally, a learning capability is needed to capture and accumulate the information derived from the various analyses, and make it accessible to the appropriate staff at all times. This requires the staff to have different types of skills. Some staff members need to be highly technical in order to conduct analyses, while others need to have architectural skills to assess the state of the infrastructure and the impact on the compromised individual products. The initial staff would need to be augmented by about 8 to 10 FTE.

In many instances, the required level of technical expertise can only be found at the vendor of the product or technology. This dependency will motivate vendors to set up a Product CERT.

The third stage of a CERT demonstrates a more proactive and preventive behavior. Leveraging the available knowledge, the CERT should become active in promoting awareness and motivating its constituency to apply security measures. At this stage, both the desire and need for organization-wide, and even sector-wide rules and regulation, and the incentive for sharing and exchanging security related information emerge. Indeed, the desire for coordinated research on threats and vulnerabilities to get ahead of the power curve of security attacks grows too. In short, the need for a Coordinating CERT and potentially a Thematic CERT becomes apparent.

Resource requirements would have to change accordingly. Some of the highly specialized technical skills can be provided by a Product CERT. Raising awareness of the wider constituency about security issues requires communication skills more than technical skills. At this stage, the staff would need to be further augmented by four or five FTE who are more business-oriented.

In the fourth stage, CERTs are connected into a network of collaborating CERTs, sometimes only within a single industry. These connections may be coordinated by a Coordinating CERT or linked through a Thematic CERT. At this stage, the collaborating CERTs will be developing what can be achieved by their combined capabilities. Considerations of task specialization are likely to occur.

At this stage, resources will be required to act as liaisons to all the various parties to which a CERT is linked: peer-CERTs, Coordinating CERTs, Thematic CERTs, and Product CERTs. This will require a further increase in resources, depending on the density of the CERT-network.

3. Trends that Increase the Need for CERTs

The operations of organizations are influenced by developments in technology and, as a consequence, in society. This section briefly discusses a series of current technology trends, including their impact on society, and a number of specific cyber security trends.

3.1. Technology Developments

- **Outsourcing** has been a theme in ICT-operations for some time. In general, the opportunities offered by outsourcing are considered from a financial perspective: moving commodity tasks to organizations that offer financial benefits (often labor costs). However, relying on the software, hardware and security procedures of a third party introduces risks that are not easy to manage. If the service providing party is compromised, this might also affect its customers. Even if the internal ICT infrastructure of only one customer is affected there can be a chain effect to the service provider and other customers. Despite the clear agreements on quality of service in service level agreements including security, reflecting the required level of trust, the outsourcing organization cannot apply its own level of rigor in risk and vulnerability analysis, security audits, and protective measures. Mechanisms must be developed to ensure that service providers will always match or outperform the security requirements of their customers.
- **Cloud services**, especially file sharing services, have become popular. The ease of use of cloud services for end-users presents a new risk to an organization's ICT infrastructure and information policies. The use of processing services, like Software as a Service (SaaS) and Platform as a Service (PaaS), or file sharing services in the cloud can easily allow confidential information to be leaked outside an organization. In order to prevent unauthorized distribution of information outside an organization's borders, specific measures must be taken to control access to cloud services.
- **Mobile devices** such as tablets and smart phones have become ubiquitous and allow staff to work from any location, including their homes. These devices have various pieces of software embedded and hold a considerable amount of data. Organizations are considering ways to handle them. Strategies like Bring Your Own Device (BYOD) allow employees to bring whatever device (and software) they personally prefer into the organization's ICT infrastructure. More limiting strategies like Choose Your Own Device (CYOD), which

allows employees to select a device from a limited pre-selected set (sometimes including software), are also being implemented. Each strategy will require its own level of security measures in order to ensure that confidential information and private information are not shared in unintended ways. Due to their nature, these devices can be used outside organizations physical borders, rendering traditional (physical) security measures less effective.

- **Big Data** is a trend resulting from increasing bandwidth and storage capacity at increasingly lower prices. Big Data allows for the discovery of patterns in large collections of data, using statistical techniques. These large volumes of data present a new and valuable asset to both organization and malicious actors alike. Big Data is a new concept that needs to be incorporated in the security policies of an organization. Organizations also need to be aware that others may be collecting Big Data about them. Therefore, information sharing policies need to take this new trend into account as well.
- The **Internet of Things** is emerging as a result of increased connectivity, underpinned by the power of IPv6. Connectivity has increased enormously and has become more and more wireless, using intelligent protocols from the IEEE 802.11-family. Where the traditional Internet is being used in the information realm, the Internet of Things allows for the control of physical objects, ranging from industrial components, like pumps and valves, to washing machines at home, and even parts in cars, such as cruise control. This trend will not only raise new challenges for organizations to address, but will also encourage a discussion on the boundaries of cyber protection. Questions like: 'Is the role of a CERT limited to its parent organization or should its constituency be extended to the individual civilians?' will need to be addressed.

In general, organizations continue to become **more dependent** on their ICT infrastructures, which have become **more complex** and **more connected** to other parties. In fact, the role of ICT has evolved from a traditional one – supporting existing manual processes – to one right at the heart of operations. Today, many operations in business and the military cannot be conducted without a reliable ICT infrastructure. This introduces new challenges and growing impacts on the operations of organizations.

3.2. Cyber Security Trends

- There is a global increase in awareness of large-scale cyber incidents, as discussed throughout this volume. This is partly due to better detection and information sharing, and partly because the technical means for attacks have become more widely available. The threshold to carry out a cyber attack is now much lower since it is easier to use attack tools, thus decreasing the required skill level of attackers. There are even professional cyber criminals that offer their services and guidance on the Internet–this is cyber crime as a service.
- There is also an **increase in the sophistication of cyber attacks**. This does not mean that each attack is more complex; rather that existing tools for cyber attacks are being developed further and are becoming more sophisticated and more difficult to counter. As a consequence, tools for detecting and handling cyber threats have shorter life spans and need to become more flexible to

allow for more dynamic responses and continuous updates. Another consequence of this increased sophistication is that attribution is becoming even more difficult. This is especially true for so-called Advanced Persistent Threats (APTs) carried out against governments and large companies, often for espionage purposes.

- In many organizations, managers (C-level) have come to recognize that cyber security is **not only a technical issue**. They have become aware that in many respects it is cheaper to develop and adopt preventive measures, than employ repair measures, including public communication, after the breach. It has also become clear that such measures need to be implemented structurally rather than as a one-time effort. There is also more pressure from a company's environment—customers and business partners are demanding trustworthy collaborations, and governments are beginning to introduce regulations that require management action on this topic. Management has also become more aware of insider threats and the fact that current and former employees, who can no longer be trusted, can breach security relatively easily.

4. Effects on Cyber Operations

The trends discussed above result in significant challenges for all organizations connected through cyberspace. Not only have threats grown in number, scope, and sophistication, but even elements in ICT infrastructures have become increasingly diverse and pervasive, and, most importantly, organizations are increasingly dependent on a flawless functioning ICT infrastructure.

4.1. Urgent Need for CERTs

The need for specialized and dedicated units that can respond to cyber security incidents has been evident for quite some time, both at the enterprise level and at the (inter-)national level. Considering the fact that fighting and recovering from cyber incidents cannot be successful as an isolated effort from one organization or even from a single nation, it is very valuable that EU leadership as well as NATO leadership devotes so much effort to stimulating and facilitating the establishment of CERTs by their member states. The recent trends only emphasize the urgency for widespread development of CERTs at all levels of society.

- At the enterprise level, organizations have realized that achieving cyber security is more than a technical problem, and that it requires managerial action and oversight throughout the entire organization as much as rules and software solutions. Effective security has to synthesize organization-wide prevention and mitigation measures, and not only rely on IT professionals working in a vacuum to 'fix' a breach after the fact.[5] CERTs can provide proactive and reactive functions, but also preventive and educational services for their constituency within an organization.
- At the national level, there is a clear need to create Coordinating CERTs that can support and facilitate national industry and other governmental bodies in establishing more dedicated Servicing and Thematic CERTs. Many EU and

NATO countries (EU: 23 of 28, NATO: 22 of 26)[6] already have national CERTs in operation, albeit at various levels of maturity.

- At the international level, EU and NATO member states are connected across borders via EU and NATO networks. This calls for governmental Servicing CERTs that protect governmental networks and systems, and prevent the dispersion of attacks to fellow member states. There are also a significant number of countries that have established governmental CERTs (EU: 24 of 28, NATO: 23 of 26).[7] NATO and the EU have an important role to play in establishing a Coordinating CERT that can support both governmental CERTs and national CERTs in member states.

4.2. Continuing Challenges for CERTs

The trends discussed previously challenge Servicing CERTs' ability to operate as a reliable support group. Some of the most significant challenges are:

- **Budgets** – In today's financially austere situation, the heavy workload can easily overwhelm the team. CERTs must find additional help outside their team, for example, at Product CERTs or specialized commercial Servicing CERTs.
- **Changing technological environment** – Also exacerbated by budget pressure, a CERT's innovative ability to keep up with adversaries' fast-evolving technological capabilities is being contested.
- **Skill levels of staff and retention** – Retention of qualified experts is also being challenged, mostly because the high demand for such specialized skills offers interesting opportunities outside CERTs. Maintaining the skill level of the current CERT's members is also ever more challenging, due to the increasing diversity of devices in the ICT infrastructure and the increasing sophistication of incidents.
- **Information sharing, accuracy, and proprietary risks** – A main challenge for Coordinating and Thematic CERTs is the increasing need to share cyber security-related information with a growing audience. This requires standardized and trustworthy approaches for information exchange (e.g. mechanisms, formats, and procedures). Although this may seem to be a relatively simple technical issue, there is the deeper lying, rather complex issue of trust. This leads to questions such as: 'can and should all security related information be shared? Are all CERTs willing to share information? Can all partners be equally trusted?' In some cases, CERTs are not allowed to share information because they may end up disclosing companies' confidential information, which could put them in an unfavorable position (e.g. disclosing ISPs' weak levels of security performance), or cause them to breach privacy rules (e.g. ISPs information sharing with law enforcement agencies).
- **Clarity in coordinated action responses** – Coordination of action is another big challenge for Coordinating CERTs. The area of operation and the mandate of a Coordinating CERT are not always clear because of the complexity of the stakeholder network and the growing number of stakeholders. This creates significant operational risks.

- **Uniqueness of some responses by product, region, sector, or state** – For a Product CERT, the challenges are in part comparable to those of a Servicing CERT. The benefit of a Product CERT is that it can focus on a (family) of product(s) or a single technology. The disadvantage is that it will have a more diverse customer base to serve. The workload of a Product CERT will most likely increase due to the demands of Servicing CERTs for external specialists. However, since Product CERTs provide commercial services, budget issues are less applicable in a growing market.

4.3. Next Steps

In order to overcome these challenges, CERTs would need to focus increasingly on a more specialized service portfolio, driven by their objectives and constituencies, and the urgency of the services they need to provide.

- **Focus on a 'First-Aid' CERT** – This type of in-house Servicing CERT would focus more on services that mitigate the possibility of a cyber incident and those that provide 'first aid' in case of a cyber emergency, typically driven by objectives like Detection, Containment, and ICT resilience.
- **Outsource analysis and repair** – Analysis and repair services could be outsourced and conducted by specialized and trustworthy cyber security service providers like Product CERTs.
- **Outsource information gathering** – Information gathering services could also be outsourced, typically to Coordinating or Thematic CERTs. By focusing on a smaller set of objectives, an in-house Servicing CERT can dedicate its resources to more advanced functions, such as predictive detection and dynamic repair.
- **Improve internal security for device and patch management** – In-house CERTs should reinforce their proactive services by improving their security tools (e.g. for secure device management) and executing patch management in a timely fashion.
- **Improve in-house risk analysis, product certification tools, and monitoring** – In-house Servicing CERTs should conduct risk analyses and product certification tests to continue developing a more resilient ICT infrastructure.
- **Emphasize information and event sharing with other CERTs in the sector and the region** – Information sharing within a collaborating network of CERTs should remain an important task for in-house Servicing CERTs. In some organizations, the units that conduct the more internally focused operational tasks are called Information Security Operations Centers (ISOC) or Computer Incident Response Teams (CIRT). As a result of the smaller services portfolio, the resource requirements can become more relaxed.
- **Emphasize information and skill sharing with whole supply chain** – Detection and containment services will require highly skilled staffs to be continually informed on ICT infrastructure's threats and vulnerabilities and current detection technologies. The size of the staff could, however, be reduced from that needed for a full service portfolio. Part of the available budget could and should be invested in developing trustworthy agreements

and liaisons with suppliers. The need for specialized technical support can in part be fulfilled by external relationships with more highly skilled CERTs, such as Product CERTs. Since they focus on their proprietary products and technologies, such CERTs will not be able to handle incidents in their customers' ICT infrastructures in a holistic manner. This need may over time give rise to outsourced Servicing CERTs that support in-house CERTs according to a contractually agreed service level. Such **commercial Servicing CERTs** would be incentivized to maintain a high level of technical expertise. However, they would need to invest in gathering information about their customers' specific ICT infrastructure and architecture, and make arrangements to ensure that this knowledge remains confidential and current.

- **Prepare for diversifying CERT landscape** – Some CERTs should specialize on a smaller set of objectives, such as Identification and Business Continuity. CERTs may assume a coordinating role and concentrate less on hands-on services (like the coordination of handling individual incident in an organization). In that case, it would act on a higher level of coordination by maintaining a network of CERTs and other cyber security related parties, where responsibilities and mandates for action are well defined. An important element of such a network will be the level of trust in sharing information, primarily to enable members in the network to be more proactive. Another important element will be support for business continuity by mediating arrangements for disaster recovery. Ideally, this CERT will offer cross-domain consultancy, sharing lessons learned and guidelines for Responsible Disclosure.

The evolution of the CERT landscape will include non-profit and for profit firms providing awareness building, education, and training. Coordinating CERTs could provide these services in cooperation with their networks; however, it is more likely that they will be provided by commercial companies specialized in education and training. Some **Thematic CERTs** already exist as specialized CERTs with a focus on a specific business or technology theme. It is expected that more of these CERTs will emerge, like the Abuse Information Exchange between ISPs in The Netherlands, or the Anti-Phishing Working Group (APWG) in the United States, or the Info Sharing and Analysis Centers (e.g. the European FI-ISAC). The greater number of such CERTs will emphasize the need for trustworthy information exchange, as well as the need for coordination networks of CERTs and the likes.

Product CERTs can be seen as a form of specialized Servicing CERTs. It is expected that more vendors will establish some sort of Product CERTs, thereby highlighting again the need for trustworthy information exchange and coordination.

Refinement of CERTs' service portfolios will encourage an increased need for collaboration and information sharing among CERTs. This will require organizations to establish relationships with various trustworthy partners. A Coordinating CERT (e.g. a National CERT) could play an important role in promoting, establishing, and maintaining such relationships.

5. Trust, the Key Factor

Information sharing, outsourcing, product certification, training, and all other types of collaboration in the cyber security realm must be bolstered by mutual trust. Several

studies, including Capgemini's own research,[8] show that if there is no or insufficient trust between participants, there will be little chance for successful collaborations.

5.1. From People to Organizations

In the early phases of a CERT, relationships among individuals create a network of trust. The existing informal networks between CERTs have demonstrated to be very effective and should not be abandoned, even when CERTs evolve and the workload increases. However, from a managerial perspective, it is not reasonable or prudent to assume or even expect trusted partners to be able to offer help 24/7, for 365 days a year. Therefore, at some point, trust held in people needs to be transferred to organizations as the more dependable, yet more anonymous entities. Replacing individuals with organizations is a delicate process, where several aspects need to be taken into account.

When establishing **trusted information sharing** relationships, a CERT should consider its objectives and constituency in order to identify and limit both the information that can and should be shared and the audience with whom to share it. In fact, communities of interest (COIs) can be set up around specific themes. This is typically how some of the Thematic CERTs were created. When sharing information, all participants must accept the mechanisms of mutual sharing (e.g. '*quid pro quo*' is a long standing principle in the Intel domain) and act accordingly.

As a result of Multinational Experiment 7 (MNE7), an Information Sharing Framework (ISF) for Collaborative Cyber Situational Awareness (CCSA) is being developed and implemented by the Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)—a new organization involving governments, industry, and the military.[9] This is a very promising development since this framework has gained broad support from entities like European Network, the Information Security Agency (ENISA), the Department of Homeland Security (US DHS), and the Internet Engineering Task Force (IETF).

When establishing **trusted collaborations**, CERTs and their constituencies should consider a set of critical conditions:

- Parties should convincingly demonstrate a strict policy of integrity concerning each other's confidential information. This calls for mechanisms like compartmentalization of information.
- Parties should, pre-crisis, agree on a service level describing how to respond to incidents. This may vary from providing advice only, to making active changes to the customer's ICT infrastructure. Although in a commercial context the incentive for providing the services is money, the agreement must allow for action when required, and for a financial settlement after the fact.
- The service provider should be very transparent in its actions. The customer should be able to review and inspect the facilities at any time.
- The service provider should maintain a permanent staff, dedicated to specific customers. The staff should demonstrate a high level of skills and knowledge, with a proven track record.
- The service provider should deliver quality results. Such results should not only focus on handling incidents, but they should also include proactive measures. Action reports should include remedial actions, and show successes in protecting customers' ICT infrastructure.

Trust is slowly gained, but can be quickly lost. In any collaboration, there will be moments of misunderstanding, below par performance, or expectations otherwise unmet. There is no prescription for what is acceptable and when the line, when crossed, is crossed irreversibly. The key is to maintain an open communication and act on facts. When sharing information or collaborating to counter security incidents, parties need to rely on the fact that behind the formalism of an organization there is still an individual responsible for the functions carried out.

5.2. Need for Enforceable Agreements and Trust-Reinforcing Institutions

In societies, organizations use contracts and formal agreements between them to create a mutually acceptable and defined level of trust. These agreements clarify the mutual obligations for the (bilateral or multilateral) parties involved. They also provide a means of pressure for settling affairs after the fact, if obligations are not honored as agreed.

While sound legal arrangements may be attainable at a national level, they are also necessary at the more challenging international level, where Internet borders have yet to be established. Supra-national organizations can and should play a vital role in solving legal arrangements issues.

Another mechanism for building trust between entities is obtaining the endorsement of a neutral organization that aims at building trust between parties in the cyber security domain, like the Forum of Incident Response and Security Teams (FIRST) and Trusted Introducer (TI). The endorsement of these organizations (e.g. certification at different levels) presents an objective assessment against pre-set criteria of the way CERTs handle information and security incidents, and protect themselves against security incidents.

5.3. Reinforce Professional Ethics

Despite all the recommended measures described above, services are ultimately delivered by people, or at least performed under the responsibility of people. Legal arrangements and technical measures are important between organizations, but they can never fully replace the ethics of individuals. Perhaps, it would be useful to introduce a form of 'Hippocratic oath' for cyber security experts, such as: 'I swear that I shall always try to the best of my ability to maintain the health of the ICT infrastructure that has been entrusted to me and always share my cyber security knowledge with my fellow oath-takers for free.'

Recommendations and Conclusions

Organizations are becoming more and more vulnerable to cyber security incidents, due to their increasing dependency and complexity of their ICT infrastructures and connectivity to other parties.

At the same time, cyber incidents are growing in scope, sophistication, and frequency. These trends and the inherent nature of the borderless Internet call for the urgent creation of national and governmental CERTs to be part of the EU and NATO member states' network of CERTs, if they do not yet exist.

The trends result also in a growing workload for existing CERTs, thus calling for better responsiveness and more adaptability. CERTs can only meet these challenges if they focus on a smaller portfolio of more advanced services, while being able to depend more and more on trusted partners for services they cannot provide themselves, and reliable sharing of security related information.

Trust is the key factor for successful collaborations and information sharing in the cyber security domain. Trust must be built carefully, at first between individuals and later between organizations. Active measures must be taken to establish a network of trusted partners and foster each individual relationship. Independent third parties can play an important role in this task. The cornerstone in any relationship will remain trust between people.

References

[1] European Network and Information Security Agency, 2012. Deployment of Baseline Capabilities of National/Governmental CERTs - Status Report 2012, Verison 2.0. [online] Available at: <http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012> [Accessed 15 October 2013].
[2] West Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., and Zajicek, M., 2003. Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.
[3] Carnegie Mellon University, 2002. CSIRT Services. Software Engineering Institute. CERT Coordination Center. Stelvio bv, The Netherlands; PRESECURE Consulting GmbH, Germany. [online] Available at: <http://www.cert.org/csirts/services.html> [Accessed 15 October 2013].
[4] IT-ISAC. About us. [online] Available at: http://www.it-isac.org/#!about/c4nz [Accessed 18 October 2013].
[5] Spidalieri, F. 2013. One Leader At A Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat. [online] Pell Center for International Relations and Public Policy. Available at: <http://www.salve.edu/Media/Website%20Resources/pdf/pellCenter/pell_center_one_leader_time_13.pdf > [Accessed 15 October 2013].
[6] European Network and Information Security Agency, 2013. Inventory of CERT activities in Europe. [online] Available at: <http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe> [Accessed 18 October 2013].
[7] Ibid.
[8] Capgemini Nederland, 2013. Nationale Cyber Security Strategie, Analyse en Vooruitblik.
[9] Multinational Alliance for Collaborative Cyber Situational Awareness, 2013. Information Sharing Framework (ISF) for Collaborative Cyber Situational Awareness (CCSA), Version 2.2.

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-97

Standards for Cyber Security

STEVE PURSER
European Union Network and Information Security Agency (ENISA)

Abstract. Standards play a key role in improving cyber defense and cyber security across different geographical regions and communities. Standardizing processes and procedures is also essential to achieve effective cooperation in cross-border and cross-community environments. The number of standards development organizations and the number of published information security standards have increased in recent years, creating significant challenges. Nations are using standards to meet a variety of objectives, in some cases imposing standards that are competing and contradictory, or excessively restrictive and not interoperable. Other standards favor companies that are already dominant in their field. The European Union, with the support of ENISA, has started to include standards in its strategies and policies, but much remains to be done. The development and use of standards is necessary, timely, and requires the involvement of public and private sector actors working in tandem.

Keywords. Cyber security standards, national security strategies, European Union, cyber resilience, standard development organizations, standardization process.

Introduction

This paper explains why standards are important for cyber security, and especially for customers with stringent security and resilience requirements, such as defense organizations. Because they are so important, it is critical to consider both the benefits associated with adopting cyber security standards and the many challenges they present. This paper reviews some of these challenges before offering an overview of several key European Union (EU) initiatives in this area, and a short summary of the work that the European Union Network and Information Security Agency (ENISA) has carried out since 2009 on standardization. The paper concludes with a number of recommendations for enhancing the effectiveness and efficiency of cyber security standardization.

1. Background

In the recently published Cyber Security Strategy of the EU, 'the EU reaffirms the importance of all stakeholders in the current Internet governance model'[1] and reiterates its support for a multi-stakeholder governance approach. This is critical because the multi-stakeholder approach is fundamental for the development of successful standards, particularly in the area of cyber security, where private sector service providers are extensively involved in carrying out the implementation of public sector requirements.

A number of EU governments are now advocating a wider adoption and use of open standards. The UK government, for example, recently published a set of open standards for data and document formats and software interoperability for the government's IT specifications.[2] Open standards also play an important role in the EU's Digital Agenda. As stated by the European Commission's Vice President Neelie Kroes: 'Open standards create competition, lead to innovation, and save money.'

What is valid at the governmental level and in the EU often applies to other countries as well. The virtual world does not observe national borders, has no uniform legal system, and does not have a common perception of security and privacy issues. It is however, relatively homogenous in terms of technology.

The standardization activities of the private sector in the area of network and information security (NIS) tend to be driven by areas of work that are in line with the core interests of product developers or service providers (i.e., authentication, billing, etc.). Aligning public sector goals with standardization priorities of the private sector remains challenging.

Despite the difference in standardization priorities, both public and private sector information security practices can be improved by identifying and responding to evolving risks and technology developments. In particular, the time lag between the appearance of a new technology or technically driven business model and the availability of applicable standards is still too long.

2. Importance of Standards in Information Security and Cyber Defense

There are many reasons why standards play an important role in improving approaches to information security across different geographical regions and communities. Some of the more important reasons include:

- Improving the efficiency and effectiveness of key processes;
- Facilitating systems integration and interoperability;
- Enabling different products or methods to be compared meaningfully;
- Providing a means for users to assess new products or services;
- Structuring the approach to deploying new technologies or business models;
- Simplification of complex environments; and
- Promoting economic growth.

Standardizing processes and procedures is an essential part of achieving successful cooperation in a cross-border or cross-community environment. In the absence of standardization, both processes and communication can be rendered ineffective. An illustrative example is provided by the way in which different countries would react to a significant cyber incident. Here, in line with the principle of subsidiarity and the need to preserve sovereign state control, decision-making is made in a distributed environment and the processes that support this procedure must be optimal. Standardization would help ensure that various countries can interact with each other according to one set of procedures.

Similarly, standards such as ISO 27001[3] encourage the adoption of a standard organization structure, which makes it easier for customers to understand how processes work, and reduces the costs of auditing and due diligence. This is largely due to the fact that these organizational standards provide a blueprint for setting up a

management system for security, but also a blueprint for auditing and checking compliance of an organization to security best practices.

Standards play a key role in ensuring that security products can be put together into systems capable of detecting and responding to real events. In particular, standard interfaces and protocols make systems integration much simpler and allow products to interoperate in heterogeneous environments. Standardization of testing methods also makes it possible to compare security products in a meaningful manner ('benchmarking') and provides a means for the end user to assess new products or services. For instance, the level of compatibility of cryptographic modules with the FIPS 140-2 standard[4] (which is used to accredit such products) is used to assess the ability of such products to meet certain security requirements.

Standardizing the approach to deploying new technologies and business models helps reduce the complexity of the business environments that deploy them, which in turn makes it easier to secure the resulting environment. Although there is also an argument against such standardization, notably that any vulnerabilities associated with such systems would also be 'standardized,' opening the door for rapid, large-scale attacks. The usual way of dealing with this, however, is not to avoid standardization but rather to ensure that the defenses used to protect information systems are not critically dependent on a single system or type of system – this is the principle of defense in depth.

Last but not least, the use of standards encourages information exchange between developers and is likely to result in greater competition between companies developing products.

All these factors have a great impact on the overall preparedness of governments to counter the cyber threat. Standardized technologies and approaches enhance harmonization among cooperating countries, and ensure a larger pool of available experts and a higher level of knowledge of systems deployed.

3. Standardization Challenges in Cyber Security

Despite the fact that an appropriate use of standards is clearly beneficial in achieving a strong approach to security in a cross-border environment, there are also many challenges to achieving this in practice.

3.1. Organizational Challenges

Over the last ten years, a plethora of standard development organizations (SDOs) has been created. These organizations have been mostly initiated by industry (Oasis, W3C, Open Data Center, IETF, Adobe, ITIL and many others). This was partially an industry reaction to the large investment in terms of time and people required by 'traditional' SDOs[5] (such as the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union (ITU)), and partially the result of convergence where standardization traditionally focused on a specific sector (e.g. IEEE, MPEG, etc.) found applicability in many others. The number of SDOs and the number of published standards has increased, which can be a source of confusion for end-users.

3.2. Areas of Standardization

Industrial interests in standardization activities in the area of NIS tends to be driven by areas of work that are in line with the core interests of service providers (for example, authentication, billing, etc.). Although an increased general interest in the area of privacy is observed, specific interest of industry is expected to diminish, as privacy-enhancing technologies are perceived as being in conflict with commercial expectations.

At the time of writing, there is no single, continuous 'line of standards' related to cyber security, but rather a number of discrete areas which are the subject of standardization:

- Technical standards;
- Metrics (related mostly to business continuity);
- Definitions; and
- Organizational aspects.

Some areas are potentially over-standardized. There are several standards on information security governance and risk management.

In some areas standards are lacking, for example there are relatively few standards that address compliance with privacy and data protection legislation. Similarly, there are not many standards covering service levels, or more broadly, service agreements and service contracts, terms of use and conditions, etc. A quick look across the different offerings of cloud providers shows that every provider has a different (often long) legal text describing the terms of use and exceptions to obligations.

3.3. Lack of Agility

Designing and agreeing on standards is a lengthy process which is measured in months (in the best cases) to years. The information technology (IT) landscape, on the other hand, evolves rapidly. In order to remain useful, standards need to evolve at a comparable pace. Failure to do so will result in standards that are either obsolete or only partially applicable to real life environments.

One solution to this issue may be to use 'good practice' documents as precursors to standards. Such documents would be subject to change control procedures that are much less stringent than those applied to candidate standards and could therefore be developed to maturity more quickly. Good practice documents that are sufficiently mature could then be used as a basis for a corresponding standard.

3.4. Competing Sets of Standards

In some areas of information security there are several different groups of standards that are defined. To some extent, these standards are competing with each other for adoption and it is often difficult for the end user to judge which is best for their particular requirements. Occasionally, it is necessary to mix and match standards from different families in order to achieve the goal. For instance, when implementing Public Key Infrastructure (PKI), it is not unusual to see organizations adopt a combination of standards (for example X.509 (ITU) for the certificate format, PKIX (IETF) standards for core PKI and PKCS (RSA) standards for interfacing to secure devices).

3.5. Economic Considerations

Although some providers see their use of recognized standards as a unique selling point, there are also many cases of companies with a dominant position, who insist on their own proprietary standards and fail to constructively support and implement standards for their products. For instance, the fact that every mobile phone vendor uses different charger plugs is annoying for consumers, and wasteful in terms of resources. In order to resolve this situation, the EU had to take action to force vendors to adopt a single standard universal mobile phone charger plug.

Companies with a dominant position have few incentives to adopt interoperable standards, because it would only reinforce the position of their competitors. For a dominant vendor there are advantages to using proprietary standards, because they lock the customer in. This lock-in means that:

- The customer cannot buy or integrate compatible products from competitors, which generates more revenue for the provider.
- It is hard for customers to switch to another supplier, because they cannot easily move their data and processes to a competitor.

3.6. Lack of Awareness

Despite the clear disadvantages associated with the use of proprietary standards, there are still many examples of cases where customers (also in government organizations) fail to demand open standards. This may well be due to a lack of awareness.

4. EU Initiatives

4.1. The EU Cloud Strategy

Last year, the European Commission (EC) published its cloud strategy, entitled 'Unleashing the Potential of Cloud Computing in Europe.'[6] The strategy aims to improve the adoption of cloud computing in Europe so as to drive innovation and reduce costs in the EU's digital market. The main issue the cloud strategy is trying to address is the fact that the digital market for cloud services in the EU is currently fragmentized. In different countries public procurement processes use different requirements. On one hand, this means that it is hard for government bodies to get what they need because cloud providers do not change their offerings for small, individual customers. On the other hand, this fragmentation hinders the development of a EU cloud industry catering to Europe's need, because it is hard for providers to build one service and sell it to government bodies in different countries. A second goal of the strategy is to leverage the combined value of public procurement in the EU to improve adoption of cloud computing in the private sector as well. The cloud strategy has three key actions:

- Better use of Standards—the goal of this action is to gain a better understanding of the existing cloud standards landscape, and foster the adoption of standards and the development of voluntary certification schemes. As part of this activity, ETSI is asked to prepare a detailed map of standards,

and ENISA is asked to support the development of voluntary certification schemes.

- 'Safe and Fair Contract Terms and Conditions'—the goal of this action is to address issues with the legal framework around cloud computing, for example in regard to data protection, and derive more standardized and simpler contract terms and conditions for cloud computing services.
- 'Establishing a European Cloud Partnership to drive innovation and growth from the public sector'—the general idea is to agree on common requirements for procurement and use them to improve market offerings and speed up public procurement of cloud computing. Security and privacy requirements play an important role here.

All three actions are closely related to standardization of technology, requirements, and procurement processes.

ENISA is currently contributing to the EU cloud strategy action that maps existing cloud standards, and is also supporting the EC in deriving a list of certification schemes as a first step to supporting voluntary certification schemes as a way to improve trust in cloud computing services.

4.2. Open Standards in Information Communications Technology (ICT)

In June 2013, the Commission published the guide 'Against lock-in: building open ICT systems by making better use of standards in public Procurement.'[7] Although not specifically related to security, this recent EU communication underlines the need for a wide user of open standards in ICT. Open standards prevent lock-in of customers, and in this way both reduces costs and fosters competition and innovation in ICT. The communication argues that open standards could save an estimated one billion euros a year.

4.3. Cyber Security Strategy of the European Union

The European Commission published the Cyber Security Strategy of the European Union (EU CSS) on February 4, 2013.[8] This strategy provides a harmonized framework for the evolution of three different aspects of cyber security, which until recently had been evolving independently. In so doing, the Commission recognized and responded to the need to bring different communities together to improve the approach to cyber security across the EU, and laid the foundations for a more coordinated approach. The Cyber Security Strategy of the EU also includes a proposal for a Directive on Network and Information Security (NIS), which would require Member States (MS) to have minimum NIS capabilities in place, and cooperate and exchange information within a dedicated network, and demand the private sector to adopt NIS enhancing actions. The Strategy contains the following assertions:

- The EU reaffirms the importance of 'commercial and non-governmental entities, involved in the day-to-day management of Internet standards.'
- 'A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establishing voluntary EU-wide certification schemes building on existing schemes in the EU and internationally.'

- The Commission will support the development of 'security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing.'[9]

Under strategic objective four, the Commission asked ENISA to 'develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardization bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.'

This is a timely recommendation as the new ENISA mandate provided the Agency with a more proactive role in this area. The new ENISA regulation in this area tasked ENISA to 'support research and development and standardization, by facilitating the establishment and take up of European and international standards for risk management and for the security of electronic products, networks and services.'[10]

There are also recommendations for public and private stakeholders. In particular, the Commission encouraged public and private stakeholders to:

- 'Stimulate the development and adoption of industry-led security standards, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers;' and equip 'new generations of software and hardware with stronger, embedded, and user-friendly security features.'
- 'Develop industry-led standards for companies' performance on cyber security, and improve the information available to the public by developing security labels or kite marks helping the consumer navigate the market.'

An important part of the Cyber Security Strategy is the proposal for a Network and Information Security (NIS) Directive. This Directive asks the Member States to support standardization in the area of NIS:[11]

- 'Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues.'
- 'Standardization of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at the EU level. To this end, it might be necessary to draft harmonized standards.'

Additionally, article 16 on standardization states the following:

- '…Member States shall encourage the use of standards and/or specifications to networks and information security.'
- 'The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.'

4.4. Cyber Security Coordination Group

In 2011, following a request of the Commission, the Standards Development Organizations CEN, CENELEC, and ETSI created the CEN–CENELEC–ETSI 'Cyber Security Coordination Group' (CSCG) to provide strategic advice in the field of IT security, Network and Information Security (NIS), and cyber security (CS). The main objectives of the CSCG are to:

- Establish a European standardization roadmap in the above mentioned areas.
- Act as the main point of contact for all *questions* by EU institutions related to standardization issues.
- Define and propose to the Commission a cooperation strategy between the EU and the US for the establishment of a framework, relating to standardization of cyber security.

ENISA has participated in and contributed to the activities of CSCG since its launch. Currently, the members of CSCG are working towards creating a first white paper addressed to the Commission, with strategic advice on priorities for R&D of EU funded research in this area, and ways to optimize EU research with mandates for cyber security standardization.

5. ENISA & Standardization

One of the tasks of ENISA, as put forward in its founding regulation, is to 'track the development of standards for products and services on Network and Information security.'[12]

Since 2009, ENISA has been identifying and elaborating on the work performed by standardization bodies (such as ISO, ETSI, ITU, CEN, CENELEC) relevant to its areas of work. One of the first deliverables in this area was a review of the state of standardization on the resilience of communications networks,[13] which at that time was not being addressed by the key standards development organizations other than as guidance for management processes. The report summarized and presented a number of findings covering the importance of correctly defining resilience in the context of standardization, the identification and presentation of the major activities undertaken by SDOs in security, and identification of key areas where further work is necessary.

Among other issues, the report also highlighted the lack of a consistent taxonomy for cyber security that identifies the role of resilience. ENISA therefore followed up on this initial report with a second one that provided an ontology of resilience alongside and embedding a taxonomy of resilience.[14] This study introduced two tools for understanding resilience as a network design target, and the output of those tools when applied to resilience. The tools introduced were classification using taxonomy, and relationship modeling using ontology with taxonomy at its core. This work was taken on board by the Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN) group of ETSI for possible future inclusion in a standard.

In addition to the work on specific areas, ENISA also facilitates cooperation between relevant EU actors (SDOs, EU organizations, industry), in order to address the shortcomings of standardization efforts. One way to achieve this would be through the promotion of best practices at the level of EU Member States through SDOs. In this particular case, ENISA would act as the interface between private and public sectors as well as interfacing with the SDOs.

ENISA has established working collaborations with SDOs and specific working groups (WG), such as ISO SC27 (collaboration agreement), ETSI (memorandum of understanding), CEN and CENELEC (collaboration agreement), and ITU SG17 (informal collaboration). These agreements allow for, among others:[15]

- 'ENISA's participation as observers in, and if appropriate, chairing of identified technical committees, their working groups, and workshops to support the preparation of European standards'.
- Evaluation of relevant ENISA research results by SDOs 'and their transfer to standardization activities'.
- 'The dissemination and promotion of information on publications, results, meetings, and seminars'.
- 'The provision of mutual support on promotional activities and in establishing industrial contacts and research networks for network and information security standards-related tasks'.
- 'The organization of topical workshops, conferences, and seminars addressing technology and research issues related to network and information security standardization activities'.
- 'The exchange of relevant information on topics of common identified interest.'

Finally, ENISA has also responded to the World Wide Web Consortium's (W3C) call for comments on the final draft of the HTML 5 specification by performing a security analysis of the standard, and making specific recommendations regarding security flaws and the security and privacy of APIs in the standard.

Recommendations and Conclusions

The following general recommendations on development and the use of standards can help NATO Member States in many areas critical to cyber security and cyber defense. These range from standardization processes and enforcement of regulations, to definition of effective practices for verification of security in national security relevant systems, to identification of standards for specific R&D areas. Recommendations are as follows:

1) Policy-makers should continue to encourage vendors to agree on the use of standards, and encourage both private and public sector organizations to include references to these standards in procurement processes.
2) Governments should incorporate standardization as part of their national cyber security strategies. Emphasis should be given to improving the coordination between policy and operational levels, and enhancing the role of public-private partnerships in standardization processes.
3) National Regulatory Authorities should make greater use of standards as a point of reference in enforcing regulations.
4) Public institutions involved in the funding of research and development should identify consistent sets of standards for different research areas. Where appropriate, publicly funded research should require compliance with these standards.
5) Standards Development Organizations should work together to identify ways of speeding up the standards development process for cyber security related standards. This might be achieved by a 'fast track' mechanism.
6) Governments of cooperating countries should work together to define a broad certification scheme allowing end users to verify that services or products upon which they rely comply with security standards.

Specific recommendations targeting resilience against cyber threats:

7) Work items should be actively promoted in the SDOs (e.g., through a mandate) to support the specification of metrics, and supporting test and validation criteria to be used in resilience (derived, where possible, from existing metrics used in the assessment of reliability and failure analysis).
8) Work items should be actively promoted in the SDOs (e.g., through the means of a mandate) to support the development of taxonomy for resilience.
9) SDOs should ensure that resilience aspects are addressed systematically in ICT-related standards.

References

[1] European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final). Brussels: European Commission. [online] Available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> [Accessed 17 November 2013].
[2] UK Cabinet Office, 2012. Open Standards Principles – for software interoperability, data and document formats in government IT specifications. [online] Available at: <http://ofti.org/wp-content/uploads/2012/12/46907_Open-Standards-Principles-FINAL.pdf> [Accessed 17 November 2013].
[3] International Organization for Standardization, 2005. ISO/IEC 27001 Information technology. Security techniques. Information security management systems. Requirements. [online] Available at: <http://www.iso.org/iso/catalogue_detail?csnumber=42103> [Accessed 28 October 2013].
[4] National Institute of Standards and Technology, 2001. FIPS PUB 140-2 Security Requirements for Cryptographic Modules. [online] Available at: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf> [Accessed 28 October 2013].
[5] Investments required by SDOs are usually very demanding in terms of time and human resources. The development of a standard, indeed, can require years of discussions, multiple drafts, and various work meetings. It is almost impossible to quantify the exact time spent developing a standard, but ISOs usually spend an average of 6 years to issue a standard, and ETSIs about 4.
[6] European Commission, 2012. Unleashing the Potential of Cloud Computing in Europe (COM(2012) 529 final). Brussels: European Commission. [online] [Accessed 17 November 2013]. Available at: ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf>
[7] European Commission, 2013. Against lock-in: building open ICT systems by making better use of standards in public procurement (COM(2013) 455 final). Brussels: European Commission. [online] Available at: <http://www.austria.gv.at/DocView.axd?CobId=52046> [Accessed 17 November 2013].
[8] European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN(2013) 1 final). Brussels: European Commission. [online] Available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> [Accessed 17 November 2013].
[9] Ibid. Cybersecurity Strategy of the European Union.
[10] Council of the European Union, 2012. Proposal for a Regulation of the European Parliament and of the Council concerning the ENISA. Council of the European Union. [online] Available at: www.statewatch.org/news/2012/oct/eu-council-enisa-position-14865-12.pdf> [Accessed 17 /11/2013]
[11] European Commission, 2013. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final). Brussels: European Commission. [online] Available at: <http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf> [Aceessed 17 November 2013].
[12] ENISA, 2004. REGULATION (EC) No 460/2004 of the European Parliament and of the Council [online] Available at www.enisa.europa.eu/?came_from=http%253A//www.enisa.europa.eu/activities/res-old/technologies/std/std> [Aceessed 17 November 2013].
[13] Gorniak, S., Saragiotis, P., Ikonomou, D., Cadzow, S., de Couessin, C., Mueller, A. and D'Antonio, S., 2009. Gaps in standardisation related to resilience of communication networks, ENISA study. [online] Available at: <http://www.enisa.europa.eu/publications/archive/gapsstd> [Accessed 28 October 2013].
[14] Vlacheas, P., Stavroulaki, V., Demestichas, P., Cadzow, S., Gorniak, S. and Ikonomou, D., 2011. Ontology and taxonomies of resilience, ENISA report. [online] Available at: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology/ontology_taxonomies> [Accessed 28 October 2013].
[15] European Unition Network and Information Security Agency (ENISA), 2013. Cyber Security Collaboration Agreement Between ENISA and European Standardisation Bodies, CEN and CENLEC. [press release] Available at: <http://pr.euractiv.com/pr/cyber-security-collaboration-agreement-between-enisa-european-standardisation-bodies-cen-and> [Accessed 17 November 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-107

A Model For Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factor, and Leadership

WILLIAM PELGRIN
Center for Internet Security

Abstract. Virtually every aspect of modern life is shaped by advancements in technology. While there are undeniable benefits to this ubiquitous use of technology and the Internet, we must also understand the security risks that come with them and take appropriate measures for preparedness. The challenges faced by government, industry, and academia continues to grow in volume and complexity as cyber security threats constantly evolve. The need to ensure that cyber security best practices are ingrained in everyone's behavior and continue to be an essential component of business operations has never been greater. Good cyber security is built on layers – a defense in depth strategy. A critical component of this strategy is to improve our cyber hygiene through positive change in behavior. The paper explores innovative ways to influence long lasting outcomes in three areas: cyber security strategy, human factor, and leadership.

Keywords. Baseline assessment, controls, cyber security strategy, experiential learning, human factor, information sharing, leadership, metrics, prioritization.

Introduction

Cyber security is now part of the mainstream consciousness. The vast majority of us have not just heard or read about cyber threats but, sadly, have also been a victim of a cyber incident. These incidents include credit card compromises, data breaches, scams, phishing, identity theft—the volume is overwhelming. Being a cyber victim is almost a rite of passage. No single segment of society is immune – individuals, corporations, governments, and nations are all under constant attack from cyber criminals. Cyber criminals encompass a diverse demographic as well – teens, hacktivists, hackers, nation states, and terrorists.

Cyber security threats know no geographic or demographic boundaries; public and private sector organizations alike face the same challenges. Potential impacts of cyber-related incidents include the disruption of essential services and critical operations or worse, that of property and loss of life. Cyber security can seem overwhelming to many, especially in light of a depressed global economy in which resources to defend against threats are scarce. It is difficult to know what to do or where to begin, especially for those lacking experience or resources. Often it is the start that stops most of us.

With our increased awareness about cyber risks, one would have thought that by 2013 everyone would be employing good cyber hygiene in order to protect themselves.

Unfortunately, we are not. Our behaviors have not changed significantly in light of the current threats. Internal processes have not embraced cyber security as an integral part of the business function. Too often technology is seen as the solution versus a tool that can be used to more securely protect information assets.

Many of the issues and concerns about cyber security threats and mitigation strategies that were being discussed ten years ago still hold true today. Too many organizations do not require strong passwords, users are insufficiently trained, systems are not patched, and users are still not cautious about clicking on links. These basic minimum-security layers, which would dramatically improve our cyber security environment, have not been universally adopted.

Approaching cyber security in a tactical, rather than strategic, manner is essential to effectively addressing these challenges. The general tendency is to discuss, analyze, and debate the same security issues repeatedly, without actually coming up with actionable measures. These behaviors have to change. Good cyber security practices must be as second nature as buckling a seat belt. Although 100% security cannot be attained, promoting positive behavioral changes minimizes cyber risks.

The need to ensure that cyber security is ingrained in users' behaviors and continues to be an essential component of operations has never been greater. Moving toward a more secure posture, however, remains difficult due to an ever-changing threat landscape. Therefore, organizations need to perform constant monitoring and assessments to answer the question 'Is my organization more secure today than it was yesterday?'

Effective metrics are necessary to inform decisions about good cyber security practices and ultimately to create a more secure environment. Measurements require first and foremost the establishment of a trusted environment in which to capture and assess metrics. Building a culture in which people can safely and accurately evaluate their organization's network is necessary. The status of an organization's network cannot be effectively measured, nor can progress be attained, if employees fear that an accurate picture of its security posture may lead to criticism, or worse. Creating this new culture starts with the principle that the assessment process cannot be about who to blame, but rather must identify what gaps exists in the system and what a roadmap to achieve an improved security posture should look like. Metrics are essential tools for organizations. Traditionally, metrics have been used to measure past performance (i.e., did the organization achieve what it planned to achieve? How well did the organization perform?). While this is one method of measuring success, it is by nature retrospective.

Metrics can also be used prospectively in order to promote positive change. The ability to affect decisions and behavior has a long lasting positive impact on improving an organization's cyber security posture. As stated by Douglas Hubbard in *How to Measure Everything: Finding the Value of 'Intangibles' in Business*:

> *If a measurement matters at all, it is because it must have some conceivable effect on decisions and behavior. If we can't identify a decision that could be affected by a proposed measurement and how it could change those decisions, then the measurement simply has no value.*[1]

The paper highlights innovative ways to use metrics to change behavior in order to improve long lasting outcomes in three areas: cyber security strategy, human factors, and leadership.

1. Cyber Security Strategy

The ability to secure critical infrastructure from cyber attacks begins with a strategy. An organization typically spends a significant amount of time planning, researching, discussing, and designing strategies before choosing one. This does not diminish the value of planning—it is still an important process—but the tendency to over-plan may reduce its effectiveness. Indeed, by the time a plan is implemented, the infrastructure and threats may have already changed, rendering the chosen strategy insufficient to address the ever-changing landscape.

An effective strategy needs to be focused on deliverables by taking tangible steps toward a common approach to improve the cyber security posture. Getting down to business means knowing what those steps are and carrying them out.

Many good cyber security strategies already exist. Organizations need to identify the one(s) that works best for their environment and implement them. A good strategy must be realistic and implementable. Incremental adjustments to its complexity can provide achievable and measureable outcomes.

1.1. A Case Study on Developing a Cyber Security Strategy

A chief security officer for a large and diverse state government with more than 60 agencies and nearly 200,000 employees implemented a state-wide cyber security strategy across all agencies, using International Organization for Standardization (ISO) controls to increase the security posture of the state. In order to facilitate the successful implementation of the strategy, the controls were categorized into four levels of criticality so that agencies could incrementally address each level. Level 1 represented critical defenses; Level 2 focused on defensive readiness; Level 3 encompassed defensive planning; and Level 4 addressed security training and awareness. Compulsory timeframes were established for the implementation of Level 1 policy requirements, due to the nature of the items in this category. Implementation of Levels 2-4 was completed in phases. This approach improved the overall state security posture and is now being leveraged at a national level.

1.2. Recommendations on Leveraging Existing Cyber Security Strategies

Long-term plans must be flexible to address the ever-changing threat landscape. They should also focus on one to three year deliverables. These deliverables should be implemented and adjusted as needed. The strategies below can serve as a launching pad for any organization to improve its overall security posture.

Existing organization and national guides already offer actionable measures that can facilitate the broader use and application of a technology or a process to promote security. In particular, the Australian Government developed a document entitled ‘Strategies to Mitigate Targeted Cyber Intrusions’[2] and indicated that at least 85% of targeted cyber intrusions could be prevented by following four mitigation strategies:

- Use application whitelisting to help prevent malicious software and other unapproved programs from running.
- Patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers.
- Patch operating system vulnerabilities.

- Minimize the number of users with administrative privileges.

Of the four strategies above, the last three can be implemented in a relatively short time.

There are a few additional measures that can be implemented along with the previous ones, and are derived from the 'Critical Security Controls' strategy published by the SANS Institute:[3]

- Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers;
- Secure configurations for network devices such as firewalls, routers, and switches; and
- Security skills assessment and appropriate training to fill gaps.

2. Baseline Assessment and Prioritization

Long term plans must be focused on deliverables. The first deliverable of any good cyber security strategy should be an inventory of critical infrastructure assets or a baseline assessment. More often that not, an organization does not know what the composition of its enterprise is because new technologies, applications, and products are layered onto existing systems. If an organization does not know its assets, it cannot protect them.

> *In many circumstances, enterprise network administrators are not fully aware of what assets (service instances on network hosts) they have nor how these assets depend on and interact with one another. Therefore, administrators lack understanding of the roles network assets play towards supporting the missions of the enterprise. Consequently, administrators are unable to identify which assets are most critical and whether or not any resiliency is present (e.g., load balancing or failover) to protect those assets in the face of failures or attacks. Therefore, network administrators do not always know how best to proceed if an asset or network failure occurs, and security teams are unaware of which assets are in greatest need of security protection and monitoring.*[4]

A complete inventory that is updated frequently is thus essential to knowing what comprises an organization's critical services and assets, and knowing the information security and other controls that are in place to protect them. Once the inventory is completed, it is possible to determine the importance and dependencies of specific critical services and assets, their vulnerabilities, and the potential threats they face. An organization can then prioritize a list of controls that would have the greatest impact in improving the risk posture against those threats.

In short, dividing the tasks into prioritized deliverables should be the starting point of any effective strategy. Similar to how a hospital prioritizes its emergency response by triaging patients and treating the most serious cases first, cyber security must be handled similarly. Although this approach may seem elementary and obvious, many organizations do not employ it at all. A divide-and-conquer approach facilitates an effective strategy and builds a sense of accomplishment that can be easily quantified.

2.1. A Case Study on Baseline Controls

The Center for Internet Security (CIS), an international not-for-profit organization, recently handled a case involving multiple state and local governments in which the failure to inventory systems and prioritize patch management—a baseline policy—had a significant impact on their networks. Attackers were able to exploit unpatched vulnerabilities in twenty-two systems, gaining a foothold into various networks. At least one incident resulted in the compromise of an entire network, including domain controllers. Some systems were compromised for up to eight months after a patch had already been released. In each of these instances, a regular patching schedule would have improved the security posture as well as avoided the costs associated with remediation.

2.2. Recommendations on Baseline Assessments

In order to develop a comprehensive approach to information security, the first step must be to inventory critical infrastructure assets. The second step should be to use assessments and scans to identify the vulnerabilities with the greatest risk, and start addressing those first. An organization that fails to fix the most urgent vulnerabilities preemptively will still have to address them after a breach has occurred and incur even greater costs for remediation.

2.3. A Case Study on the Use of Metrics to Assess Progress

A large state implemented a report card system to measure and rate progress against common standards. This was a valuable component of its cyber security program. Each year, report cards were issued to all agency executives during a cyber threat brief, along with a review of the results from the year's compliance activities. Metrics were compiled using visual graphs representing the various areas of the policy with the relative compliance percentages for each agency. Report cards were issued to each agency measuring its yearly progress, and metrics were provided to show where each agency stood in its progress relative to all other agencies and the statewide average. These report cards were not issued as punitive measures and were explicitly drafted in such a way that no agency would be blamed for not meeting a specific deliverable. Many factors were taken into account to rate an agency's compliance with the standards. The focus was clearly placed on positive recognition where objectives had been met, on identifying gaps in compliance to the policy, and providing recommendations on how to close those gaps. The creation of this safe environment resulted in the participation of all agencies.

A certificate of excellence, signed by the Governor, was then issued to each agency that achieved overall policy compliance during an annual executive briefing for all agency commissioners. This recognition spurred healthy competition among the agencies and improved the overall state security posture.

Strengthening an organization's cyber security posture, however, entails much more than getting a grade once a year and filing a report away on a shelf. This is an on-going process that requires executives and security staff to work together to review progress and have candid discussions to identify issues and solutions. In the example above, every agency came into substantial compliance within a short time. The report card allowed agencies to measure their progress against security standards, enabled

them to track compliance over a period of time, and helped them rate their progress relative to their peers.

2.4. Recommendations on Measuring Progress

The following recommendations will help organizations conduct a baseline assessment, track trends and patterns, measure progress, and encourage compliance:

- Establish concrete, measurable, and attainable metrics.
- Implement an incremental approach toward a more secure cyber posture.
- Create a report card process to encourage and track compliance.
- Compare results through the report card process across different organizations and reward success through recognition of achievements. This metrics methodology has proved itself as a motivator and healthy competition that encourages organizations to improve faster.
- Use metric questions, such as those found in the National Cyber Security Review (NCSR).[5]

3. Timely and Actionable Information

There has been much talk about the importance of information sharing. The end state of information sharing, though, is not just the sharing itself. Information shared must be both timely and actionable. Out-dated, non-actionable information is unhelpful. All too often information is not released until every last detail is checked and rechecked. Although this is important to avoid overlooking important details or misinterpreting significant factors, perfection is the enemy of the good. It is critical to disseminate credible information as soon as possible. Information can always be qualified with a disclaimer, indicating that what is being shared is the preliminary or best information at the time of distribution. Threat actors will most likely already have all the information anyway. Delaying distribution will only withhold it from those who need it most.

3.1. A Case Study on Timely and Actionable Information Sharing

During a recent incident handled by CIS, timely and actionable intelligence had a significant positive impact in the overall response. An advanced persistent threat (APT) group targeted twelve critical infrastructure entities via a phishing email campaign (Sykipot malware). CIS immediately contacted those twelve entities and, after further analysis, identified what is believed to be the source from which the actors obtained the addresses—a publicly posted document containing hundreds of email addresses of individuals working in these critical infrastructure organizations across the country. CIS notified all the organizations and shared the indicators with the federal, state, and local governments. A number of the critical infrastructure entities reported back to CIS that they had identified the attack using the indicators shared via CIS bulletins and remediated the potential incident before significant damage occurred.

3.2. Recommendations for Timely and Actionable Information Sharing

The following are basic recommendations to guide effective information sharing practices:

- Ensure that the information being shared has real value and is not just a recompilation of something else.
- Ensure that analysis and action steps are tailored to specific audiences. Gearing products specifically to the intended audience will greatly enhance their value.
- Develop key partnerships. Public-private partnerships, as well as collaborations between civil and law enforcement sectors, must be established in advance and constantly reinforced. Knowing whom to call when there is a crisis is half the battle.
- Start to identify gaps in the organization's contacts and then immediately develop working relationships with those who will be critical in a crisis.
- Be willing to give more than you get. You can't break down barriers if you are territorial yourself.

4. The Human Factor

User behaviors can have a significant impact on the security of an organization's environment. Symantec's 2013 Internet Security Report stated that two out of the top three causes of data breaches in 2012 were attributable to human error (accidental disclosure, theft or loss of equipment).[6]

It would be a mistake to assume that every employee understands his or her individual responsibility for securing cyberspace. A sizable percentage of the workforce does not believe that they are responsible for the security of their organizations' networks, and many of them may have not received appropriate cyber security training. Addressing the human factor is a critical defense strategy for improving an organization's security posture.

Many of the recent high profile breaches, in which millions of records have been impacted, were the result of human error. In one case, for example, the breach was due to an employee falling prey to a phishing scam and clicking on a link in a malicious email. The ramifications were magnified by the use of weak passwords and unencrypted data.[7] In another case, an employee clicked on a malicious link in an email that had already been caught by the company's spam filter. Thus, the individual made a number of bad decisions, from retrieving a suspicious email out of the spam folder to clicking on an unknown link in that email.[8]

Understanding how to incentivize cyber hygiene and promote good behavior begins with the recognition that all actions have consequences. In the cyber security arena, one rarely sees a tangible and direct correlation between actions and their consequences. Only in the movies does clicking on a malicious link result in the computer screen going black and the hacker's face appearing right after. In the real world, nothing immediately blows up, melts, or looks different after you click on untrusted links, insert a thumb drive containing malicious code, or open a bad attachment. Trying to change unsafe behaviors is difficult because there are no immediate obvious negative consequences.

An effective measure to significantly improve user behavior is to employ a more experience-based approach in which individuals experience the lesson in a tactile way.

4.1. A Case Study on Experience-based Approach to Safe Cyber Security Practices

A major exercise was able to test this tactile-based learning experience through a large-scale mock phishing attack involving 10,000 employees across multiple agencies. With the consent of the agencies' commissioners, two separate emails were sent to employees enticing them to divulge passwords on a linked website. The objectives were to assess communications and establish whether they positively influenced desired behaviors – specifically whether written directives that clearly identify the problem, discuss the risk and specify appropriate action, have any meaningful impact on behavior.

The exercise was conducted in three stages:

- Phase 1: An advisory bulletin was emailed to employees from each agency's chief informing them about phishing scams – what they are, how to avoid them, and in particular why it is critical not to reveal sensitive information such as passwords.
- Phase 2: Approximately two weeks later, the phishing exercise was launched. This consisted of an email sent to the same set of employees, appearing to come from the agency's information security officer, and asking them to enter their user identification and password into a new 'password checker' tool.

If the employee entered his or her user ID and password, the exercise would end and a message would appear informing the employee that this was a phishing exercise and, had it been real, they would have just been hacked. Too many employees fell for the scam. Those employees immediately received remedial training and a quiz to help them recognize a phishing scam attack.

- Phase 3: A month later, another phishing exercise was launched to the same set of employees to see if the tactile approach made a difference in their behavior. The second phishing email came from a bogus department in their agency requesting the employees to click on a link and complete a survey. The metric consisted of identifying: who fell prey to the scams; did they already fall prey to the first one; did they learn anything and do better on the second exercise?

The number of people who fell prey to the second phishing scam decreased by nearly 50 %. When employees were surveyed as to why they fell for the phishing scam, they indicated that they did not realize they were engaging in inappropriate behavior, even though they had read the advisory before the exercise was launched. Therefore they needed to have that tactile experience to understand and see the relationship between bad behaviors and falling prey to a scam in order to change to a positive behavior.

Other phishing exercises, both in the public and private sectors, have been conducted with similar results. As part of these exercises, information about positive behaviors in cyberspace was clearly conveyed to everyone, including that the right approach to avoid falling prey was to have strong passwords and not to click on untrusted links. What was missing, though, was the direct linkage between the action and the consequence. It is important to state that even with the tactile approach, one experience is not enough. Repetition is important in sustaining positive behavior, for it is only through repeated lessons over time that we will permanently change for the better.

The consequence of poor security choices was not readily apparent as a result of the bad behavior and, therefore, was not sufficient to convince the user to change it. In hindsight this makes perfect sense. If one clicks on a malicious link but does not see any negative consequence of this action in the immediate short term, why would that behavior need to change? Rarely does a message appear on a computer screen announcing the machine has been hacked. In fact, in some of the most successful cyber attacks, the victim never knows that they have been breached and that a cyber criminal has obtained full access to the computer with all rights and privileges. Suppose the computer physically combusted into flames when a user clicked on a bad link—then the user would most likely think twice before clicking in the future.

In the phishing exercise described above, the tactile approach seemed to have the biggest impact, providing a deeper and more meaningful understanding of consequences of actions. That immediate and direct relationship between what one does and its effect is very powerful.

4.2. Recommendations on Fostering Positive Behavioral Changes

The following are basic recommendations to address the human factor of cyber security and incentivize end users to adopt positive behaviors:

- Make it clear that cyber security is a shared responsibility.
- Understand that everyone will not do the right thing all the time.
- Expect and plan for the unexpected.
- Recognize that the human factor plays an important role in the security of the organization.
- Do not rely only on verbal or written communications or directives, especially where critical operations are involved.
- Address the human factor by changing behaviors through a tactile approach.
- Reinforce tactile learning through repetition.
- Be creative in communication and training techniques – making a situation real and demonstrable is essential for learning.
- Connect the dots between actions and the consequences. This provides tremendous motivation for changing behavior positively.

5. Leadership

If there is to be true behavioral change, it has to come top-down from the boardroom level. Leadership is essential in promoting positive change. In order to encourage leaders to become champions of cyber security, it is critical that the issues are presented in a clear and understandable manner. Plain speaking about how to protect, defend, respond, and recover from cyber security incidents can go a long way toward getting leaders to embrace and support the mission. A digital dashboard, for example, is a useful tool that helps visualize complex issues and events, enabling insight to lead to action. Dashboards have become increasingly important for management of complex data across diverse organizational areas, and can help leaders visualize information that will greatly assist their ability to make improved decisions.

The reality, however, is that most public and private sector senior leaders are not cyber security experts, suggesting that something as abstract as cyber security can be overwhelming and hard to grasp. There are no crystal balls as to the when, who, how,

where, and what of an attack. Visualizing these hard-to-grasp issues through a dashboard makes them more real, more readily understood, and promotes positive behavioral change. Additionally, dashboards can quantify over time the progress that an organization has made to a more secure state.

5.1. A Case Study on Using Dashboards to Visualize the Cyber Environment

An exemplary model of a secure dashboard used by an organization contained cyber security information occurring across different organizations and sectors. A major feature included an interactive mapping function that maps actual cyber attacks and depicts the location of attacks from source and destination. Networks and systems linked to critical infrastructures, including utilities, communication, finance, energy, and transportation, are at greatest risk. These systems have shifted from stand-alone air-gapped systems to Internet-connected ones. Consequently, the threat posed by determined bad actors has grown.

By implementing the dashboard, leaders can begin to see potential threats occurring in other jurisdictions that may have otherwise gone unnoticed in their organization. Using a geographic information system interface would enable an organization to overlay both man-made and natural events. The importance of understanding and literally seeing the relationship between the physical and cyber domains cannot be overstated.

5.2. Recommendations on Effective Use of Dashboards

This two-step plan can help leaders better understand and visualize their organization's networks, complex issues and events, and the information needed to make improved decisions:

- Visualize the information by using a mapping technology that relates physical and cyber issues.
- If there is a cyber event occurring, create a visual representation and show how it is impacting both physical and cyber assets. This will greatly enhance the understanding and importance of the event.

Recommendations and Conclusions

Cyber threats facing organizations in both the public and private sectors will continue to increase in volume and complexity. This ever-changing environment demands constant vigilance and, while there are some sophisticated solutions, there are many simple steps organizations can take to shore up defenses. Measuring progress is essential. The key is to focus on actions, deal with facts, and change negative behaviors. The following summarizes an implementable blueprint of fundamental practices that can truly have a significant impact on an organization's ability to detect, protect, respond to, and recover from cyber incidents:

- Recognize that there is no 100% guarantee of security, but there are many layers that can—and must—be implemented to strengthen readiness and response.

- Start with understanding an organization's environment. Make a baseline assessment of the network and of what is running on it. Assets cannot be protected if they are unknown.
- Identify a strategy and cyber security standards with a minimum level of security protection and preparedness acceptable for the organization. Implement this strategy to the predefined level, raising the bar over time toward a more advanced state of protection. Make sure that the strategy includes some of the top *Strategies to Mitigate Targeted Cyber Intrusions* and the *Twenty Critical Security Controls for Effective Cyber Defense.*
- Develop a deliverable-oriented action plan. Prioritize tasks—identify, on one side, those areas of greatest need (those so vulnerable that they must be fixed regardless of the cost) and, on the other side, those that are easy and cost little or nothing to remediate, and then work toward the middle.
- Modify the strategy over time as necessary.
- Conduct a gap analysis to measure current status and develop a path forward. Implement an on-going inventory assessment and modify the approach as the threat landscape changes. Flexibility is key.
- Create a safe environment for employees that fosters actionable and timely information sharing and reporting of suspected and confirmed incidents.
- Lead by example; make sure actions clearly demonstrate a collaborative and cooperative approach.
- Recognize that any successful plan must address the human factor.
- Establish concrete, measurable, and attainable metrics to assess progress.
- Develop prospective metrics to influence positive, long-lasting behavior focused on best practices for cyber security.

References

[1] Hubbard, D. W., 2010. How to Measure Anything: Finding the Value of 'Intangibles' in Business. 2nd ed. Hoboken, NJ: John Wiley & Sons, Inc.
[2] Australian Government, 2012. Strategies to Mitigate Targeted Cyber Intrusions. [online] Available at: <http://www.dsd.gov.au/images/top35-table-2012.png> [Accessed 29 October 2013].
[3] SANS Institute, 2012. Twenty Critical Security Controls for Effective Cyber Defense, version 4.1. [online] Available at: <http://www.sans.org/critical-security-controls/> [Accessed 29 October 2013].
[4] Marshall, S., 2013. CANDID: Classifying Assets in Networks by Determining Importance and Dependencies. University of California at Berkeley, Electrical Engineering and Computer Sciences.
[5] MS-ISAC (Multi-State Information Sharing & Analysis Center), 2013. 2013 Nationwide Cyber Security Review Question Set. [online] Available at <http://msisac.cisecurity.org/resources/ncsr/documents/NCSRSimpleQuestionSetFinalkmp.pdf> [Accessed 29 October 2013].
[6] Symantec, 2013. Internet Security Threat Report, Volume 18, Annual Threat Report 2013. [online] Available at: <http://www.symantec.com/security_response/publications/threatreport.jsp> [Accessed 6 September 2013].
[7] Be'ery, T., 2012. The South Carolina Data Breach: A Lesson in Deaf and Blind Cybersecurity. [online] SecurityWeek. Available at: <http://www.securityweek.com/south-carolina-data-breach-lesson-deaf-and-blind-cybersecurity> [Accessed 6 September 2013].
[8] Litan, A., 2011. RSA SecurID attack details unveiled – lessons learned. Gartner Blog, [blog] 1 April. Available at: <http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-securid-attack-details-unveiled-they-should-have-known-better/> [Accessed 6 September 2013].

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-118

Coordination and Cooperation in Cyber Network Defense: the Dutch Efforts to Prevent and Respond

ELLY VAN DEN HEUVEL[a] and GERBEN KLEIN BALTINK[b]
[a] *National Cyber Security Centre in The Hague, The Netherlands*
[b] *Dutch Cyber Security Council*

Abstract. Effective Computer Network Defense requires close cooperation and collaboration between government and industry, science and education, national and international efforts. The Netherlands offers a concrete example of a successful public-private partnership aimed at improving overall cyber security for its society in general, including government, industry, and citizens. This requires more that a mere national cyber security strategy. Mutual trust between parties and close international cooperation and collaboration are essential. The Dutch approach has been successful so far, but it needs the constant attention and focus of all parties involved. The lessons learned from this approach can help build NATO's non-traditional networks and enhance its overall cyber defense posture through cooperation with partner countries, organizations, and commercial entities.

Keywords. Computer network defense, cyber security, Dutch approach, European Union, international cooperation, national cyber security strategy, NATO, public-private partnership, trust building.

Introduction

In his book 'Networks and States,' Milton Mueller demonstrated that traditional nation states are unable to control the Internet.[1] Despite this, the Netherlands has worked hard to improve cyber security for Dutch society in general, including government, industry, and the public services. It is clear, however, that an open, secure, and reliable digital domain can only be achieved with close coordination and cooperation between all parties involved. Other countries and international organizations are carrying out similar activities. Effective Computer Network Defense (CND) requires more than a mere national cyber security strategy. It demands cooperation between government, science, industry, and the people. To add to the complexity of the solution, this cannot be done on a national level alone. Close international cooperation and collaboration is also required.

This article addresses the current state of affairs in The Netherlands with respect to safeguarding our digital domain. It will discuss both goals already achieved, as well as the way forward.

1. Dutch Efforts to Secure the Digital Domain

We live in a very exciting time. We have entered the digital era regardless of whether we are ready. Internet banking, cloud computing, 3D printing, the Internet of Things, Google Glass™, and new digital technology in health care are just a few examples. The innovations seem endless, and while innovations can bring progress and new opportunities, they can also bring threats and new vulnerabilities.

An open and secure Internet is important for our society and economy. The benefits created by online services, however, are increasingly challenged by a variety of threats. Cyber crime, for example, is on the rise and will remain a serious problem for decades to come. In addition, both state- and non-state actors increasingly exploit vulnerabilities in the digital domain for their own (intelligence) purposes. A growing number of organizations have started to realize these dangers and have begun investing in cyber security. While the private sector has (re)acted quickly, governments appear to have only recently discovered the security aspects of cyberspace, which has resulted in a rapid growth of the number of national cyber security strategies,[2] taskforces, conferences, and publications, just to name a few. Although these efforts are commendable, they are definitely not enough to realize an effective CND.

Alexander Klimburg and his co-authors outlined recent national efforts on cyber policy development in their 'National Cyber Security Framework Manual.'[3] The text illustrates some of the best practices in this domain from different NATO member states.

This paper will focus specifically on the Dutch approach, given that The Netherlands has gone through a similar cyber security strategy development process in recent years.[4]

The Netherlands' National Cyber Security Strategy, launched in 2011, was an action plan. Focal areas in the strategy are:

- Creating the Cyber Security Council and the National Cyber Security Centre (NCSC);
- Establishing threat and risk analyses;
- Increasing the resilience of critical infrastructure;
- Increasing capacity for responding to ICT disruptions and cyber attacks;
- Intensifying cyber crime investigation and prosecution; and
- Encouraging research and education.

A few of these focal areas will be discussed in more detail to show how the Netherlands has tried to achieve improved cyber security across society.

The second edition of the National Cyber Security Strategy (NCSS2) was launched in October 2013. This is a true public-private partnership, one that involves all relevant stakeholders in an effort to improve cyber security in our society. The five strategic goals of the NCSS2 are:

- Making the Netherlands resilient against cyber attacks and able to protect its critical processes;
- Fighting cyber crime;
- Investing in secure ICT products and services, taking the promotion of privacy into consideration;
- Building coalitions for freedom, security, and peace in the digital domain; and
- Investing in innovation and having adequate knowledge levels.

It is now important for the Netherlands to evolve from public-private partnership to full private-public participation. As a country, we need to move from being aware to being capable.

1.1. Public-Private Partnerships (PPP)

Over 80% of the critical infrastructure is in the hands of the private sector. This is the main reason why PPP is essential. Since the inception of the NCSC, public-private cooperation has been established and intensified. The former Government Computer Emergency Response Team (GOVCERT.NL), established in 2002 as the CERT for the Dutch Government, has evolved into the current National Cyber Security Centre (NCSC), where many governmental and private parties, including academia, work together. A Cyber Security Council was also established, with members from industry, government, and academia. Both NCSC and the Council will be discussed in more detail below. Although all parties involved in establishing these partnerships had their own interests in being part of this collective initiative, it quickly became clear that the digital domain is so complex and so vulnerable that working together was the only feasible way to make progress. In the NCSC2, we move from partnership to participation in every possible field.

In general, we can conclude that the Dutch approach in bringing all these parties together has resulted in an improved understanding of each other's interests and needs, and it has helped better define common goals and criteria. Some of these common objectives are:

Mobilizing relevant parties in the field of cyber security;
Sharing knowledge between all parties;
Capacity building;
Developing a proactive posture to diminish crime and potential damages;
Creating a community in which cyber experts have a career development;
Learning together from incidents to create a better working environment for public-private participation; and
Increasing cyber security awareness and understanding at the boardroom level.

1.2. National Cyber Security Centre [5]

NCSC is situated within the Directorate of Cyber Security of the Ministry of Security and Justice. In addition to hosting NCSC, this Directorate also has a Policy Division that develops new cyber security policies and strategies, a unique combination of insights and expertise is very important.

In 2012, NCSC opened its doors after embedding GOVCERT.NL in this new Centre. Cyber security now officially falls under the umbrella of national security in The Netherlands. The handling of incident response is still an important and valued task, and the Centre continues to be a respected member of the international CERT community.

Although the Centre has maintained the original CERT mandate, it is more than a mere Governmental CERT plus. It reflects a new concept entirely. The main difference between the earlier GOVCERT.NL and NCSC today is that is the latter is a public-private partnership. NCSC serves not only the government, but also public and private parties within the critical infrastructure. NCSC's products and services are focused on national security. During large incidents or crises that might endanger national security,

it has an operational coordinating role as well. It is not surprising, then, that the number of employees has almost tripled in size in less than two years. NCSC adopts a pro-active approach to create a resilient environment. Computer Network Defense is at the core of its efforts. In order to achieve its objectives, the Centre is developing three public-private networks:

- A national detection network—this network would facilitate a proactive approach by detecting incidents before they occur. This would consist of a network of organizations that voluntarily share information about incidents in a safe environment. By so doing, an incident in one organization becomes an early warning for others.
- A national response network—NCSC is closely cooperating with public and private CERTs to create an effective network that could handle large incidents or calamities in The Netherlands.
- A national expertise network—this network would help bundling expertise and sharing knowledge between all the relevant parties to facilitate CND and resilience for society at large.

The development of the national detection network for the Dutch government is almost complete. Currently, the NCSC and the Council are exploring how best to involve private parties that are most relevant to national critical infrastructure. The toughest issues that need to be discussed, such as disclosure of commercially sensitive information, shared responsibilities, and cost related to the national detection network, are being addressed in open dialogues between government and industry representatives. Mutual trust is essential to achieve progress in this area.

Within NCSC, public and private parties are already working side by side to make The Netherlands more secure and resilient. Some of the various examples of cooperation include secondments to the Centre and, working collaboratively on projects or any other form that can be agreed upon. NCSC, for example, has liaison officers from all the public and private parties involved with cyber security or cyber crime, such as the High-Tech Crime Unit (HTCU), the Ministry of Defense, the financial sector and Microsoft. Working together, these actors will build a more secure cyber domain for The Netherlands. With the goal of a more secure future in mind, public and private parties get together without reference to commercial interests or government power plays. Freed from those factors, all parties involved create a community built on trust.

A governance board consisting of five to seven representatives drawn from both the public and private sectors will be appointed early in 2014. This board will oversee the NCSC annual work program, in order to make sure that the activities of the Centre meet the priorities of both parties. Members of the board will act as NCSC ambassadors.

Several Information Sharing and Analyses Centers (ISACs) are directly connected to NCSC. IT specialists from more than 12 critical infrastructure sectors already meet several times a year. The number of ISACs continues to grow. These centers are organized by sectors themselves. Representatives of HTCU, Intelligence Service, and NCSC are also present at the meetings. In between meetings, members will have on-going interactions.

1.3. Cyber Security Council

The Dutch Cyber Security Council was established after the publication of the Dutch Cyber Security Strategy. The Council was initiated by Ivo Opstelten (Secretary of the Department of Security and Justice) on June 30, 2011. The Dutch Cyber Security Council has 15 members from government, industry, and the scientific community, for a total of three scientists, six public sector and six private sector representatives.[6] The Council is supported by an independent secretariat. Thanks to its broad composition, the Council represents a significant part of Dutch society, although there are always those who feel their interests are not represented in the Council.

The Council oversees the Dutch National Cyber Security Strategy and offers both solicited and unsolicited advice to the Dutch government and society. The Council also facilitates public-private dialogue on the complex matter of cyber security—for example, by working with organizations at the boardroom level about the importance of cyber awareness and cyber defense.

The role that the Council played during the DigiNotar incident (see Section 2), for example, demonstrated the effectiveness of this kind of public-private partnership in the digital domain.

In July 2013, the Council issued an advice on the new National Cyber Security Strategy, published in October 2013.[7] The advice specifically focused on the need for close cooperation and coordination in the field of incident detection and response. Only through active information sharing, timely response and seamless collaboration can a secure digital environment be established.

The Council, which has now been in place for over two years, has clearly established its authoritative voice to actively participate in the debate about the digital domain. Through open dialogue members, often sharing the experiences of cyber incidents, have gained trust in the relevance of such a diverse Council.

The advice of the Council, a product of jointly seeking possible solutions, is now considered high quality, concrete, and focused. The different interests of the various members and the fact that beforehand no specific goals were identified (other than focusing on the relevance of cyber security) proved to be an excellent prerequisite for success. Members of the Council understand the obvious differences in their roles, responsibilities, and objectives, so that need not be a topic of discussion in itself. On the contrary, it ensures that members are aware of the primary approaches and interests of the other participants. As a result, those differences can be seen as advantageous, and have often created more consensus than was previously expected. Nevertheless, consensus is not something easily obtained—the often-stereotypical images of disagreement you might expect are quite often true. Scientists in the Council, for example, wish to have all their arguments considered in depth and believe that serious research has to be done before a particular solution can be chosen. Business representatives, on the other hand, want government to make serious budget concessions to improve cyber security, while government officials expect citizens and businesses to take their own share in creating a cyber-resilient society. Moreover, while business leaders are usually opposed to new laws and regulations, public representatives often want to impose more specific cyber rules, regulations, and supervision. Apart from these issues, all members of the Council are cognizant of the importance and urgency of addressing cyber security. This helps in creating the right focus and forces the members of the Council to collaborate on concrete recommendations.

Since its inception, the Council has issued a number of statements of advice; the most recent expressly intended to offer input for the renewed Cyber Security Strategy. This recommendation stressed the priorities identified by the Council and the importance of public-private-academic partnerships to achieve reliable solutions in the field of cyber security.

2. Lessons Learned Identified by the Cyber Security Council

Shortly after the establishment of the Council, the Netherlands was confronted with the DigiNotar crisis.[8] This incident, in which certificates were stolen from a major Dutch registrar, resulted in an (initially improvised) close cooperation between government, industry, and the scientific community. The Council became actively involved in discussing the possible actions and the necessary coordination between government, business, and society. Perhaps the most complicated issue in this incident had to do with public trust in the availability of reliable Internet connections to conduct business or share information with the government.

In-depth analysis of what went wrong at DigiNotar was not the responsibility of the Council, although reports indicated that remarkable mistakes were made, reflecting poor operational security management including the use of standard, insecure passwords and poor security procedures. The Council wanted to review this incident from a more general perspective, and therefore requested a study in 2012 by Professor Bob Hoogenboom to investigate this incident along with several others.[9]

After the study was completed, members of the Council realized that they had to put their differences aside in order to search for practical, common solutions on which they could agree. Some of the lessons learned from the incident identified in Hoogenboom's study can apply to other nations as well:

- Incidents and crises are a blessing in disguise—they act as a real 'wake-up call' for all parties involved, as well as a start for new dialogues.
- Mutual trust can be built from the actual experience of cooperation and dialogue, and confidence is enhanced by reputation.
- Taboos should become open topics of discussion within organizations and society. The boardroom level should be involved so that security becomes an issue in purchasing policies and supervision can be revisited.
- Incidents will become public: showing openness will enhance reputation.
- Cyber security is equivalent to economic security—translate cyber security into economic benefits.
- Good security is not enough, ICT is not perfect—organizations should also focus on detection and (multidisciplinary) response.
- Learning from incidents is important—discuss and convey lessons learned on many stages, inside and outside the cyber security community.
- Make sure there are no 'free riders' and emphasize the 'moral capital'[10] in responding to incidents.

Based on these conclusions and recommendations, the Council currently focuses on cyber awareness. Apart from their participation in various conferences and campaigns related to cyber security, members of the Council also visit and interact with the directors of public organizations, large companies, and industry associations. It is during these personal dialogues that the complex subject of cyber security can be

addressed most effectively. The outcomes of these discussions are usually tested for feasibility in the Council and can then serve as concrete advice for the government and industry.

Because of its unique composition and open cooperation, the Council has been very successful in implementing a true public-private partnership. However, this is still limited to the national level, so future efforts should focus on international cooperation.

3. Threat and Risk Assessment

The need to properly understand cyber threats has been apparent since the beginning to all participants in the public-private partnerships. GOVCERT.NL (later NCSC) was asked to draft an annual Cyber Security Assessment Netherlands (CSAN)[11], the first of which was published in November 2011.

In addition to drawing on the experiences from real incidents, the CSAN reports are based on a variety of underpinning data and information, and discuss the most relevant threats as seen by experts from government and industry. In general, they conclude that negative effects on ICT security are increasingly impacting the interests our society seeks to protect. In the field of cyber security, they identified four types interests that need to be protected:

Individual Interests	**Organizational Interests**
• Privacy • Freedom of speech • Access to services • Physical safety	• Products and services • Means of production, including funding and patens • Reputation • Trust
Chain Interests	**Social Interests**
• Responsibility for information of citizens or clients • Management of general facilities and systems, such as the municipal personal records database, iDeal and DigiD • Mutual dependence between organizations	• Availability of vital services • Protection of (democratic) rule of law and national security • Infrastructure of the Internet • Free movement of services

Figure 1. Key interests in the cyber domain (source: CSAN 2013)

Organizations working in cyber security must take each of these interests into account, which can be difficult given that these interests may be perceived and valued differently—even in contradiction—by different people. The following trends have been identified in the most recent Cyber Security Assessment (July 2013):

Table 1. Summary of threats, actors and targets [12]

	Targets		
Actors (threats)	**Governments**	**Private organizations**	**Citizens**
States	Digital espionage	Digital espionage	Digital espionage
	Disruption of IT (use of offensive capabilities)	Disruption of IT (use of offensive capabilities)	
Terrorists	Disruption of IT	Disruption of IT	
Professional criminals	Theft and sale of information	Theft and sale of information	Theft and sale of information
	Manipulation of information	Manipulation of information«	Manipulation of information
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover	IT takeover
Cyber vandals and Script kiddies	Theft and publication of information	Theft and publication of information	Theft and publication of information
	Disruption of IT	Disruption of IT	
Hacktivists	Theft and publication of information	Theft and publication of information	Theft and publication of information
	Disruption of IT	Disruption of IT	Disruption of IT
		IT takeover	
	Defacement	Defacement	
Internal actors	Theft and publication or sale of received information	Theft and publication or sale of received information (blackmail)	
	Disruption of IT	Disruption of IT	
Cyber researchers	Receiving and publishing information	Receiving and publishing information	
Private organizations		Theft of information (business espionage)	
No actor	IT failure	IT failure	IT failure

4. Research and Education

Based on the earlier Research Program IIP-VV (a Dutch acronym for ICT Innovation Program Security and Privacy *Veilig Verbonden*), the Cyber Security Council asked Government to combine their several departmental R&D budgets for cyber security research into a single National Cyber Security Research Agenda (NCSRA). Although initially it was a challenge to convince the different Departments to share their R&D

efforts, by the end of 2011 the first NCSRA was published and by early 2012 the first R&D projects had begun. On 4 November 2013 the second NCSRA was published, offering both academia and industry opportunities for new cyber security research projects. Where possible, these projects will be linked to ongoing or new EU research programs.

Through a *Matchmaking Event*, the organizers of the NCSRA bring together a group of specialists form industry, academia, and government to discuss the most relevant research topics and enable cooperation between different organizations in new research proposals. The initial results from NCSRA1 are promising, offering new insights as well as prototype software and methods to improve cyber security.

From the viewpoint of Computer Network Defense, perhaps the most interesting result was the integrated approach of cyber security R&D and the close collaboration between academia, industry, and government.

In establishing the NCSRA, binational efforts were made between The Netherlands and the United States of America to agree upon research agreements in the realm of security.[13] This agreement includes joint research projects in the field of cyber security.

More details on the R&D Agenda can be found at www.iipvv.nl.

5. The Need for International Cooperation

All these national efforts are part of the current strategy, but most lack the international dimension. The close collaboration within the international CERT community, unfortunately, is an exception. Although different activities can have bilateral projects embedded, or links with EU or NATO policy development can be followed closely, there remains a need for improved international collaboration. Luckily, we see that other countries and International Organizations are looking for the same.

Most countries are currently aware they have to invest in cyber security and crime prevention.

It is critical to understand that many Internet applications—over 80%—are in the hands of the private sector. This means both government and business should be involved in protecting digital assets. A strong public private partnership is one of the main pillars of cyber security. Another challenge is that the cyber domain remains divided. This cannot stand, and the walls between public and private worlds, or between security and crime-fighting organizations, must be torn down. There is also some work to do within the public and private sectors. Last but not least, international cooperation needs to be improved. This can be done with a mutual and more altruistic goal: making the digital world a safer place.

In this field we can make use of the existing network of CERTs. These CERTs or National Cyber Security Centers are not law enforcement organizations, which most of the time is very helpful in creating true international public-private partnerships. Nonetheless, CERTs will have to find ways to work together with law enforcement organizations, although there is no doubt that the cooperation between CERTs and law enforcement is only part of the solution. A great number of other parties can and must contribute to make the digital world more secure. Cyber security is a worldwide issue that transcends the capabilities of any one country. It should not be handled just by governments—cooperation between public and private parties is the key to success.

Recommendations and Conclusions

1) Vision and Focus

It is important to maintain an open and secure Internet to facilitate economic growth, innovation, scientific progress, and social and cultural interaction. It is critical to understand future developments and possibilities of the Internet and new technologies. In order to hit cyber crime where it hurts most, we need to be able to focus. Metrics, trends and threats, and other analyses are needed. A multinational Cyber Security Agenda (including research) is advisable. Computer Network Defense should not be viewed only as a national task, but rather as an international or at least multinational effort.

2) Governance and Legislation

A balanced and realistic governance framework that guaranties an open and safe Internet encourages the creativity of inventing and implementing new applications. Parties must take their own responsibilities within this framework. Additional legislation and mandates may be needed. Cyber crime is fast, the law is slow. Some of the challenges are data exchange, state responsibility, criminal cooperation, and the applicability of (inter)national law. We need a solid legal foundation for effective cooperation. This should have high priority. A security concept should enable end users to buy and use products and services that they can rely on so they are able to take their own responsibility.

It is difficult to define the appropriate roles in the digital domain for government, industry, academia, and citizens. It may seem natural to expect that the governance models of our traditional, physical world apply, but more often than not they do not.

A key recommendation for the international community working on Computer Network Defense is, then, to take the interests of all parties involved into account and to realize the opportunities that true public-private partnerships can offer. Trust and active involvement are necessary as well: in the digital domain, we all have to invest in developing new ways of working and living together.

3) Cooperation and Coordination

Cooperation must exist between and within the public and private parties. Parties that are part of an open and more secure cyber space should be able to trust each other and use each other's knowledge and strength to achieve all of the above.

It is clear that all the relevant parties have to cooperate on a national as well as international level. In the field of cyber crime and cyber security, there is a great deal of activity, but it is not always coordinated and it is not always known by others.

Strengthening and extending existing cooperation is essential to keep pace with current threats. Cooperation should take place on all levels: operational, tactical, strategic, political, and policy. Level playing fields and comparable maturity levels of the players involved are necessary to facilitate effective international collaboration.

The European and international government CERTs should maintain their effective cooperation at the operational level. A more strategic cooperation may be achieved by setting a multinational security agenda. The Netherlands is willing to initiate this cooperation.

4) Colocation

The way the cyber security capabilities in The Netherlands have been organized (colocation of the CERT functionality, operational knowledge, and expertise as well as policy development in the Directorate Cyber Security) has real advantages. The close linking between departments within government, as well as with the ISACs, academia, and industry form one well organized 'cyber capability unit', and this clearly has advantages. It is recommended that this (perhaps typically Dutch) approach be followed by other countries that are developing cyber capabilities at the national level.

5) Research and Development

Knowledge is key. Research is conducted in various countries by various institutions. The results of the research are not always easily shared. In addition, the reports are not always reliable due to the competing interests of the commercial parties. That is also why academia is an important player in the field. Easy access to knowledge is crucial to cyber security. So is innovation. Developing new tools and sharing them amongst each other is something that is needed on a structural basis. The EU should have a coordinated research agenda that is shared with other interested countries. In this way duplication can be avoided and results can be shared more effectively.

6) Capacity Building and Education

Capacity building and education are a worldwide problem. There is a dearth of high-quality cyber security professionals and leadership across the public and private sectors. There are various initiatives in the field of training and education that are mostly aimed at the mid-term. In The Netherlands, *The Hague Security Delta* (HSD) is an example of how to coordinate education and to stimulate innovation. It is an initiative of the Mayor of The Hague. Part of the HSD is the Cyber Security Academy. This academy combines existing tracks on cyber security taught at various universities. This way, a well-trained student on cyber security can become available within a few years. It also tries to connect the enterprises in this field and stimulates the start up of new small innovative enterprises. The NCSC and its partners will focus on short-term education and training for employees that are recruited and that need extra education.

In brief, Computer Network Defense requires close cooperation and collaboration between government and industry, science and education, national and international efforts. The complex character of the digital domain offers us instantaneous access to information and services on the one hand, but makes our critical infrastructure more dependent of its uninterrupted availability at the same time. Much more than in the past, government, industry, and citizens rely on critical services provided by private parties who are not limited by traditional geographic boundaries. This requires new, innovative methods of cooperation and coordination. In this paper, we have seen the possibilities that can be realized when serious efforts are made in public-private partnerships. The Dutch approach has been successful so far, but needs the constant attention and focus of all involved.

Broadening this concept to the international arena, with specific focus on NATO and EU, must be the focal point of upcoming activity in the field of Computer Network Defense.

References

[1] Mueller, L. M., 2010. Networks and States: The Global Politics of Internet Governance (Information Revolution and Global Politics). Cambridge: The MIT Press, p. 4.
[2] Luiijf, E., et al., 2013. Nineteen National Cyber Security Strategies. International Journal of Critical Infrastructures, 9, InderScience, Olney, pp. 3-31.
[3] Klimburg, A. ed., 2012. National Cyber Security Framework Manual. Tallin: NATO Science for Peace and Security Programme.
[4] Dutch National Cyber Security Centre, 2011. The National Cyber Security Strategy (NCSS): Strength through cooperation. The Hague: Ministry of Security and Justice. [online] Available at: <https://www.ncsc.nl/english/current-topics/news/national-cyber-security-strategy-launched.html> [Accessed 8 November 2013].
[5] More detailed information on the Dutch National Cyber Security Center can be found at www.ncsc.nl.
[6] Members of the Dutch Cyber Security Council: (industry) Eelco Blok, Bart Hogendoorn, René Steenvoorden, Jan van Bekkum, Tineke Netelenbos, Ben Voorhorst; (science) Bart Jacobs, Corien Prince, Michel van Eeten; (government) Dick Schoof, Rob Bauer, Jannine van den Berg, Mark Dierikx, Marc van Nimwegen, Rob Bertholee.
[7] Dutch National Cyber Security Centre, 2013. Cyber Security Assessment Netherlands. The Hague: Ministry of Security and Justice. [online] Available at: <https://www.ncsc.nl/english/current-topics/news/cyber-security-assesment-netherlands.html> [Accessed 15 November 2013].
[8] Dutch National Cyber Security Centre, 2011. Dossier DigiNotar. The Hague: Ministry of Security and Justice. [online] Available at: <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/files%5B2%5D/dossier-diginotar.html> [Accessed 8 November 2013].
[9] Hoogenboom, A. B., 2012. Lessons Learned from Cyber Incidents. The Hague: National Cyber Security Council. [online] Available at: <www.ncsc.nl/csr/publications>
[10] The moral capital addresses the responsibility of the C-suite in taking care of cyber security before, during, and after incidents. 'Do not try to hide it from the public' Hoogenboom advised, 'but take an active approach to communicate what went wrong and inform the public about the things that will be changed to prevent similar incidents in the future.'
[11] The CSAN not only addresses threats and actors, but also indicates the possible ways to control those threats. Resilience and response are essential topics in the annual CSAN reports.
[12] Dutch National Cyber Security Centre, 2013. Cyber Security Assessment Netherlands: IT Vulnerability As High As Ever. The Hague: Ministry of Security and Justice. [online] Available at: <https://www.ncsc.nl/english/current-topics/news/cyber-security-assessment-netherlands-it-vulnerability-as-high-as-ever.html> [Accessed 8 November 2013].
[13] The Agreement between the government of the United States of America and the government of the kingdom of The Netherlands on cooperation in science and technology concerning homeland and civil security matters was signed in 2012.

Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

doi:10.3233/978-1-61499-372-8-130

Conclusions

MELISSA E. HATHAWAY[a] and JOHN N. STEWART[b]
[a] *Council of Experts, Global Cyber Security Center (GCSEC)*
[b] *Cisco Systems and*
Council of Experts, Global Cyber Security Center (GCSEC)

Information Communications Technologies (ICT) are at the core of the Internet infrastructure and embedded in our society today. Countries are seeing ICT benefits in multiple online services, including e-banking, e-healthcare, e-government, and e-learning. With a steadily increasing number of online services, the Internet infrastructure becomes more and more important. In short, today's society no longer only uses these online services and Internet infrastructure, it relies upon them. Yet, both are vulnerable to a growing number and increasingly malicious breadth of cyber activities. For example, intellectual property and personal information are illegally copied, online and critical services are disrupted electronically, systems are erased or destroyed, and sophisticated malicious cyber actors are able to operate without detection for quite some time.

The North Atlantic Treaty Organization (NATO) sees these malicious activities as a strategic threat and is acting to help the global community strengthen its cyber defenses. In 2011, NATO adopted a new cyber defense policy that articulated a clear vision of how the Alliance plans to improve its cyber defense posture. NATO understands that it must improve its capacity for Computer Network Defense (CND) and adopt effective practices for incident detection and response, especially with regard to national networks that NATO relies upon to carry out its primary mission of collective defense and crisis management. Additionally, NATO is using its Science for Peace and Security Programme (SPS) to address emerging security challenges like those presented by malicious cyber threats.

In September 2013, NATO SPS sponsored an Advanced Research Workshop, entitled "Best Practices in Computer Network Defense (CND): Incident Detection and Response," to exchange expert knowledge in cyber defense and discuss approaches and solutions to this emerging security challenge. Participants were selected from industry, academia, and public institutions who have direct hands-on experience with and responsibilities for incident detection and response. They brought a multinational and multidisciplinary perspective from sixteen countries and three international institutions and shared their experience, knowledge, and positions on CND. Together, they generated twenty-one specific findings and nearly a dozen technical papers to help improve NATO member states and partners' cyber defense posture. The ten chapters in this book represented their expert research and technical insights that will continue to advance CND and inform NATO's cyber defense policy.

The book's initial chapters described a wide range of issues and set the stage regarding the scope and complexity facing operators and decision makers in the CND field. Chapters 1 and 2 presented a summary of findings and new threats and trends in CND. The following three chapters detailed the current state of the art in advanced incident detection, mitigation, and response technologies and processes, and helped

show the technology gaps between what is in place today versus what can be achieved. The remaining five chapters turned to policy, practice, and measurement. Chapter 6 explained how national strategy plays a key role in CND and expressed concerns regarding policy and regulation that could unintentionally make CND practices more difficult. Chapter 7 walked through the critical role of CERTs and their development and deployment to support CND mission, while Chapter 8 discussed standards and their role in effective CND. Chapter 9 demonstrated metrics and measures required to show both progress as well as effectiveness. Finally, Chapter 10 presented a case study from The Netherlands of an effective private-public partnership.

Of the many findings in these ten chapters, five findings stood apart from the others.

First, identifying critical services is more important than identifying critical infrastructures. Services, like electric power, navigation, and telecommunications transcend national boundaries. Changing the focus from critical infrastructure to critical service may change NATO's approach to protection, resilience, recovery, and restoration of assets. It may also highlight the interdependencies among organizations and nations requiring different approaches to common defense.

Second, a baseline assessment enables an organization to identify the current state of the controls it has in place to protect infrastructures, assets, and services. Once a baseline is established, it is possible to prioritize a list of the controls that would have the greatest impact in improving risk posture against real-world threats and then map progress along the path toward a future state that is more resistant, resilient, and recoverable.

Third, as we continue to invest in digitizing our infrastructures and everything behind it, security considerations must become a core component of the purchasing and acquisition decisions, and not be negotiable. Work factor analysis can help acquisition and procurement officials determine whether the vendor product or service will increase the costs for the adversary.

Fourth, commercial entities are developing, deploying, and operating advanced techniques for network defense. The technologies are accessible and affordable, and they are showing promising results. Techniques ranged from using moving target architectures to confuse the adversary to turning to the Internet Service Providers/Telecommunications Providers to provide an upstream or forward deployed defense. Other effective techniques include monitoring the dark space of the Internet. Intelligence from upstream dark space monitoring can be used to reprogram deep-packet inspection (DPI) sensors within the enterprise zone to detect zero-day activity.

Lastly, no organization should accept the status quo. Our networks are compromised and we have become accustomed to assuming that the adversary has penetrated our defenses. Because of this, many organizations have shifted their security approach toward monitoring and detection. Organizations are monitoring ingress and egress routes, cataloguing the tactics, techniques, and procedures of their adversaries to understand impact and adversaries alike. New tactics and countermeasures are available to strengthen security postures and become more resistant to cyber threats.

This publication contains actionable information to strengthen security and recommendations that, if followed, will help governments take action and reduce risks. In a domain where speed is essential, where advanced defense is required against advanced offense, and where collaboration and learning amongst defenders is essential,

keeping pace and deploying advanced process or technology is only possible when you know what is available. This report shows what is possible and available today.

Knowing what is possible and available, and doing something with it, are quite different – the latter being in the hands of you, the reader.

M.E. Hathaway (Ed.)
IOS Press, 2014

Subject Index

advanced persistent threat 30
baseline assessment 107
big data 19
building blocks 54
cloud computing 19
computer emergency response teams 81
computer network defense 19, 118
control systems 19
controls 107
critical infrastructure 19
cyber attack 30
cyber defense 54
cyber resilience 97
cyber security 19, 30, 43, 54, 81, 118
cyber security posture 65
cyber security standards 97
cyber security standards and requirements cyberspace 65
cyber security strategy 107
dark space 30
data exfiltration 30
decentralized public key infrastructure 54
decision-making 19
defense-in-depth 43
domain name service 30
Dutch approach 118
European Union 65, 97, 118
experiential learning 107
full stack security 54
Harvard architecture 54
honey things 30
honey tokens 30
human factor 107
identity 30
indicators of compromise 30
information communications technology 19, 65
information flow control 54
information sharing 81, 107
infrastructure defense 43
international cooperation 118
internet of things 19
LangSec 54
leadership 107
metrics 30, 107
micro kernels 54
misinformation 30
moving target(s) 30, 54
national cyber security strategy 65, 118
national incident response 65
national security strategies 97
NATO 65, 118
network traffic analysis 43
patching 30
prioritization 107
proactive cyber defense 43
public-private partnership 118
reconnaissance 30
security services 81
separation kernels 54
standard development organizations 97
standardization process 97
technology trends 81
telecommunication providers 43
trust building 81, 118
upstream intelligence 43
upstream security 43
verification process 54

This page intentionally left blank

M.E. Hathaway (Ed.)
IOS Press, 2014

Author Index

Gaycken, S. 54
Gijsbers, K. v
Hathaway, M.E. vii, 1, 3, 130
Holt, M.W. 65
Klein Baltink, G. 118
Kruidhof, O. 81
Lindner, F. 'FX' 54
Lindstrom, G. 19
McMahon, D. 43
Pelgrin, W. 107
Purser, S. 97
Rigoni, A. 19
Stewart, J.N. 30, 130
van den Heuvel, E. 118

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank