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].