2015

Strategic Cyber Intelligence.pdf

Randy Borum
John Felker
Sean Kern
Kristen Dennesen
Tonya Feyes

Strategic cyber intelligence

Randy Borum
School of Information, University of South Florida, Tampa, Florida, USA
John Felker
Cyber Intelligence Strategy, Hewlett-Packard Company, Herndon, Virginia, USA
Sean Kern
National Defense University, Washington, DC, USA
Kristen Dennesen
FireEye Labs, Reston, Virginia, USA, and
Tonya Feyes
TF Solutions, Washington, DC, USA

Received 27 September 2014
Revised 1 November 2014
Accepted 3 November 2014

Abstract

Purpose – This paper aims to highlight the importance and role of strategic cyber intelligence to support risk-informed decision-making, ultimately leading to improved objectives, policies, architectures and investments to advance a nation or organization's interests in the cyber domain.

Design/methodology/approach – Integration of professional research literature from the fields of intelligence studies, strategy and information/computer security.

Findings – Investing in technology, firewalls and intrusion detection systems is appropriate but, by itself, insufficient. Intelligence is a key component. Cyber intelligence emphasizes prevention and anticipation, to focus cybersecurity efforts before an attack occurs ("left of the hack"). Strategic cyber intelligence can substantially reduce risk to the organization's mission and valued assets and support its due diligence.

Originality/value – This paper describes how strategic cyber intelligence can be implemented and used within an enterprise to enhance its cyber defense, and create a more proactive and adaptive security posture. It not only describes strategic cyber intelligence as a distinct discipline, but also demonstrates how the key intelligence functions articulate with existing cybersecurity risk management standards.

Keywords Risk management, Risk assessment, Competitive intelligence, Cyber intelligence, Cybersecurity, Strategic intelligence

Paper type Conceptual paper

Introduction

The International Multilateral Partnership Against Cyber Threats (IMPACT), an alliance of 152 countries, has recognized that "cyber threats and attacks are able to strike from virtually anywhere in the world, potentially causing catastrophic social and economic harm to countries that are oceans away" (IMPACT, 2014). It is clear that risks

This article is adapted, in part, from the Intelligence and National Security Alliance (INSA) White Paper: Strategic Cyber Intelligence, developed by INSA's Cyber Intelligence Task Force in March, 2014. It contains, however, substantial original and expanded material.

Information & Computer Security
Vol. 23 No. 3, 2015
pp. 317-332

2056-4961
DOI 10.1108/ICS-09-2014-0064

in the cyber domain reach far beyond identify theft and cybercrime, to threaten national and international security (Stevens, 2013). INTERPOL notes that a global proliferation of cyber threats spans from state-based actions to those originating from non-state actors and violent extremist organizations (Noble, 2013), and nearly all international surveys suggest that the volume and sophistication of attacks are increasing. This paper focuses primarily on the USA perspective, but the overarching strategic issues are applicable to many nations and to private sector enterprises as well.

Though cyber threats are widely known, they are often poorly understood. Policymakers invoke terms like malware, malicious code, viruses and distributed denial of service (DDoS), focusing mainly on the "technical" dimension of the cyber threat. The human dimension – threat actors and their activity, intentions and capabilities – is subordinated or missed. This state of discourse would be akin, at the height of the Cold War, to focusing on plutonium-239 or weapons delivery systems. Raw materials and delivery systems are certainly relevant, but they are not decisive. Effective defense should focus on adversaries, not just on their tactics.

In January 2013, after an 18-month study, the US *Defense Science Board's Task Force on Resilient Military Systems and the Advanced Cyber Threat* offered recommendations to improve DoD systems' resilience to cyber attacks. One of those recommendations was to: "Refocus intelligence collection and analysis to understand adversarial cyber capabilities, plans and intentions, and to enable counterstrategies" DoD Defense Science Board, 2013, p. 46). Activity directed to the capabilities, intentions and activities of potential adversaries and competitors, as they evolve, in the cyber domain is cyber intelligence (Ludwick *et al.*, 2013; Office of the Director of National Intelligence, 2014; RSA, 2012). The scope of this Defense Science Board (DSB)-advised effort might be regarded as "strategic cyber intelligence" (Dennesen *et al.*, 2014).

A "flow of intelligence" exists in collection and analytic disciplines among the strategic, operational and tactical levels of an enterprise and its mission. In practice, the three levels overlap, but this "levels" framework assists agencies and organizations in directing appropriate resources and effort toward intelligence activities that support its strategic objectives (Mattern *et al.*, 2014).

Many cybersecurity discussions and warnings emphasize tactical cyber intelligence to support the "on-the-network" fight. Strategic and operational levels of cyber intelligence receive less attention (Borum *et al.*, 2014). As a result, military commanders (or senior management in the private sector) may not receive the right type of cyber intelligence to effectively inform and properly resource the organization's risk management program.

A lack of emphasis on the strategic level has posed enduring challenge security intelligence efforts in many countries, not just in the cyber domain. In the USA, for example, a Central Intelligence Agency (CIA) conference in 2004 noted:

> A major [community] weakness […] is its difficulty in providing strategic intelligence – the comprehensive overviews that put disparate events and the fragmentary snapshots provided by different intelligence sources into a contextual framework that makes it meaningful for the intelligence consumer (Central Intelligence Agency, 2004, pp. 3-4).

Nevertheless, the tactical level focus continues to dominate discussions about America's cyber defense. The definition of "cyber threat intelligence,[1]" for example, crafted by the US House of Representatives' (H.R.3523) focuses on "systems" and "networks"

instead of strategic assets such as intellectual property, trade secrets, sensitive business information and other data that contribute to an organization's competitive advantage, including brand protection. Equating cyber threats with network activity deprives operational and strategic leaders of actionable information that could help them protect the organization's valued assets.

In this paper, we highlight the importance and role of strategic cyber intelligence to support risk-informed decision-making, ultimately leading to improved objectives, policies, architectures and investments to advance a nation or organization's interests in the cyber domain.

Strategy and cyber intelligence

The strategic level of planning and control focuses on establishing an organization's mission and direction, setting objectives and conceiving plans for how those objectives will be achieved (Mattern *et al.*, 2014). Strategy is easily misunderstood:

> […] strategy is not really a plan but the logic driving a plan […] {it} furthers one's advance towards goals by suggesting ways to accommodate and/or orchestrate a variety of variables – sometimes too many for the strategist alone to anticipate and understand (Heidenrich, 2008).

Intelligence informing strategic decisions (strategic intelligence) provides context, but it does not only provide context. Though strategic intelligence is distinguishable from "current intelligence" and *tends* to focus on longer timeframes, it does not always (Heidenrich, 2008).

For every enterprise, strategy evolves and its implementation changes. The strategic intelligence analyst must monitor the path and impact of that evolution and anticipate how changes might shape strategic priorities and directions.

In 2009, at the request of The White House, the *Comprehensive National Cybersecurity Initiative* (The White House, 2009) outlined a series of broad objectives to help secure the USA in cyberspace. Major themes included shared situational awareness across US Government agencies; enhancing counterintelligence and supply chain security; and expanding cybersecurity education to prepare the next generation. The goals described in this document are emblematic of broad strategic-level, aspirational aims designed to support policy.

Strategic aims can also support operations. The National Security Agency/Central Security Service, while not publicizing its operational plans, have used the following budget categories for their prioritized activities: prevent malicious cyber activity; detect, analyze and mitigate intrusions; and shape the cybersecurity environment (Alexander, 2013). In, the US Department of Defense (2011) (DoD) released its *Strategy for Operating in Cyberspace*, describing the Department's aims to build a defensible architecture; enhance shared situational awareness and understanding of the operating picture; develop a "concept" for cyberspace operations; expand the force of personnel trained to support the cyber mission; and possess decisive capabilities to act (US Department of Defense, 2011). These aims provide the kind of guidance that can shape operations and inform allocations of fiscal and personnel resources.

For DoD, strategic cyber intelligence products can inform decisions about how best to build a defensible architecture. They can enhance shared situational awareness and understanding of the operating picture. They can help to frame a "concept" for cyberspace operations and inform decisions about creating decisive action capabilities.

Strategic cyber intelligence is well positioned to collect and process information about potential adversaries to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities or to support other intelligence activities, including integrated information and cyberspace operations (National Initiative for Cybersecurity Careers and Studies, 2013).

Scoping strategic cyber intelligence

The Intelligence and National Security Alliance's Cyber Intelligence Task Force (Mattern *et al.*, 2014) outlines defining features for each operational level of cyber intelligence based on:

- the nature, role and identity of the consumer;
- the decisions the consumer will make;
- the timeframe in which the consumer tends to operate;
- the scope of collection;
- the characterization of potential adversaries; and
- the level of technical aptitude required for cyber intelligence collection.

Accordingly, strategic cyber intelligence is:

- produced for senior leaders at the executive or "chief" level in both private and public sectors;
- used to inform the development of organizational/national strategy and policy that will direct the organization, often over the long term (more than three years);
- collected broadly within the sector to which the organization belongs and likely includes complementary sectors (e.g. R&D and manufacturing, supply chain);
- focused on threat vectors and adversaries that include nation and non-nation state actors with intent and capability; and
- generally non-technical in nature, instead focusing on inter/intra sector trend analysis, stated and unstated objectives of nation and non-state actors and other strategic indicators.

Strategic intelligence is actionable information, analyzed and produced to inform a decision or support a decision-maker. Decisions are based on choices. Analysts help to generate and evaluate those choices to reduce uncertainty. To be effective, the analyst must understand the problem, the desired outcomes and the priority and impact of unfavorable outcomes. Assessing the weight of favorable and unfavorable outcomes requires the strategic cyber intelligence analyst to collaborate with senior leaders to identify, define and prioritize the information requirements for a given decision or set of decisions.

Strategic cyber intelligence typically informs three types of decisions. Those designed to:

(1) advance an organization's aims/objectives;

(2) gain advantage; and

(3) manage risk.

Relevant to those decisions is information about the organization's assets and resources, potential threats and hazards and the operating environment and context. The specific units of information necessary for a senior leader to make informed strategic decisions are sometimes referred to as critical information requirements (CIRs). The essential elements of information will vary for different decisions, but may involve the status of existing logistics, safeguards, security posture and personnel (internal) or the tactics, intentions and capabilities of a potential adversary and the status of the operating environment (external). Also, with regard to external factors, the DSB Task force recommended specifically that cyber intelligence include information about:

- identification and understanding of adversarial cyber weapon development organizations, tools, partnerships (e.g. supply chain), leadership and intentions;
- development of targeting information to support initiatives to counter cyber weaponization; and
- accurate assessment of adversarial plans and capabilities for policymakers (DoD Defense Science Board, 2013).

Looking at these parameters, it is immediately apparent that cybersecurity is not only driven by what is "on the network". Network activity is only part of what influences operations in cyberspace, and represents only one level of cyber defense and intelligence activities in support of operations. Actions at this level are typically reactive and generally occur only after the adversary is already "inside the wire". Strategic cyber intelligence tends to focus to the "left of the hack".

Strategic cyber intelligence and risk management

Success in cyber defense and cyber operations relies heavily on identifying, assessing and managing risk in the cyber domain. Risk management is one of the overarching functions of strategic cyber intelligence. Cyber risks should not be segregated, but considered in the context of the enterprise's total risk. As such, strategic cyber intelligence either uses the organization's existing risk terminology, or through communication and awareness, adapts the culture to understand the relevant cyber terminology.

Alignment is a central, guiding principle for the strategic cyber intelligence mission, particularly in risk management. The enterprise cybersecurity objectives must be considered in the context of its available resources, potential threats and the conditions of the operating environment. Aligning these elements is a fundamental element of strategy.

A basic framework for conceptualizing and communicating about risk might focus on the following constructs, defined here based on the National Institute for Standards and Technology's (NIST) "Glossary of Key Information Security Terms":

- *Risk*: A measure of the extent to which an entity is threatened by a potential circumstance or event.
- *Threat agent*: The intent and method targeted at the intentional exploitation of vulnerability.
- *Impact*: The magnitude of harm that can be expected to result from the consequences of a threat agent successfully exploiting vulnerability.
- *Countermeasure*: Actions, devices, procedures, techniques or other measures that reduce vulnerability.

The DSB Task force conceptualized cyber risk with greater detail as a function of *threat*, *vulnerability* and *consequences*:

> The threat broke into two categories: adversary intent and their capabilities (Deter, Disrupt). Vulnerabilities are described as either inherent or operationally introduced (Defend, Detect), and consequences either fixable or fatal to the impacted systems (Restore, Discard) (DoD Defense Science Board, 2013, p. 6).

Strategic cyber risk management: roles and functions

Collaboration between strategic cyber intelligence analysts and senior leaders is the foundation for an effective risk management program. Senior leaders are the primary consumers of strategic cyber intelligence, and they must define and clearly communicate the organization's critical intelligence requirements. NIST emphasizes this point:

> To be effective, organization-wide risk management programs require the strong commitment, direct involvement, and ongoing support from senior leaders/executives. The objective is to establish strategic risk assessment and then institutionalize the appropriate risk management into the day-to-day operations of organizations as a priority and an integral part of how organizations conduct operations in cyberspace (Ross, 2011b, p. 14).

Senior leaders and executives must actively participate in aligning cyber intelligence resources with the enterprise's most critical mission and business needs. Enterprise in this context includes suppliers, partners and other members of the sector and of complementary sectors in which the organization or agency operates.

The strategic dimension of cyber risk management diverges from day to day, common security practices. Risk-based security policies are often defensive and driven by "compliance" requirements, rather than mission requirements. They focus almost exclusively on tactics for securing networks, data, applications and operating systems. A recent survey of 1,300 IT professionals in the USA and UK illustrates this narrow network-focused propensity. The Ponemon Institute (2013) asked respondents how they measured the success or effectiveness of their organizations' risk-based security efforts. The responses most often included specific, tactical metrics such as time taken to patch; number of policy violations, uninfected endpoints and data breaches; status of end user training; and amount of unscheduled downtime.

These are not strategic metrics that inform senior leaders' decision-making. Cyber-related considerations that matter in a strategic sense are the ones that impact an organization's ability to achieve its overarching mission objectives. Examples might include answers to the following:

- Does the organization operate in a high, moderate or low cybersecurity risk industry?
- What is the value of the organization's information and information flows to potential threat actors?
- What are the confidentiality, availability and integrity risks to the organization's assets?
- What legal liabilities exist related to the type of information stored, such as personally identifiable information (PII) or Health Insurance Portability and Accountability Act (HIPAA)-protected data?

If a company, for example, runs a high-volume e-commerce operation and considers availability of its Web site to be critical, intelligence related to a DDoS attack is likely of high strategic importance. Likewise, a company considering new operations in a foreign country would value cyber intelligence that helps them orient their security posture to indigenous threats.

Network metrics alone are insufficient for analyzing risk. Senior leaders must define their organizations' strategic CIRs based on the critical value of select assets and programs to operations and to the organization.

Who should the senior leader/executive look to in terms of satisfying their strategic CIRs? In the public sector, the main strategic cyber intelligence producers are the Department of Homeland Security (DHS), Department of Justice and the DoD.

In March 2013, DHS, DoJ and DoD mutually defined specific roles that each will fulfill to support national cybersecurity. The "USA Federal Cyber Security Operations Team"[2] agreement assigns DHS the responsibility to disseminate domestic cyber threat and vulnerability analyses through the National Communications and Cyber Information Center (NCCIC) and the private-sector Information Sharing and Analysis Center (ISAC) construct. Because DoJ leads all domestic national security operations, its National Cyber Investigative Joint Task Force investigates and analyzes ongoing cybercrime incidents. Finally, the DoD is responsible for gathering foreign cyber threat intelligence.

Private sector organizations with sufficient resources may develop organic cyber threat and/or business intelligence units for their strategic cyber intelligence requirements. Smaller organizations may opt to outsource to private cyber security and cyber intelligence providers and others with global access to threat information.

Strategic cyber intelligence information sharing

Private-public information sharing is an essential element of strategic cyber intelligence. In the words of General Keith Alexander, "Securing our nation's network is a team sport" that requires close collaboration between government and the private sector. This collaboration is especially critical in critical infrastructure protection because the private sector owns about 85 per cent of America's critical infrastructure (US Government Accountability Office, 2006).

A number of cyber intelligence sharing efforts have emerged. The US Government has followed recommendations of Presidential Decision Directive 63 (PDD-63), the 2009 "White House Cyber Policy Review" (The White House, 2009) and CSIS' report "Security Cyberspace for the 44th Presidency" (Center for Strategic and International Studies, 2008) to create several information exchanges. Through these programs, private sector organizations can exchange cyber threat information with peer institutions from their industry sector, and receive critical threat updates from the US intelligence community. While some challenges remain to efficient information sharing, the US Government has achieved some notable early successes.

DHS's ISAC program is an example of a successful effort to enhance information sharing with the private sector to enhance critical infrastructure security. In 1998, PDD-63 directed each critical infrastructure sector to establish mechanisms for sector-specific information sharing about sector threats and vulnerabilities. Critical infrastructure owners and operators developed ISACs as "trusted entities" to meet this requirement. There is currently a multi-state ISAC and sector-specific ISACs for energy, emergency management and response, financial services, information technology,

maritime, national health, nuclear, real estate, research & education, supply chain, surface transportation, public transit, communications and water. A retail ISAC is also developing under the auspices of the Retail Cyber Intelligence Sharing Center, sponsored by the Retail Industry Leaders Association.

DHS also sponsors the following efforts:

- The Homeland Security Information Network secure Web-based portal for information sharing and collaboration between public sector, private sector and international partners engaged in the homeland security mission.
- The Industrial Control Systems Cyber Emergency Response Team works to reduce risks within and across all critical infrastructure sectors by facilitating communication among and between law enforcement, intelligence and other governmental agencies and the infrastructure control systems owners, operators and vendors.
- United States Computer Emergency Readiness Team improves the nation's cybersecurity posture by coordinating cyber information sharing, and proactively managing cyber risks to the nation.

DHS' Office of Cybersecurity and Communications also regularly publishes several products to facilitate information sharing:

- NCCIC Weekly Analytic Synopsis Product – Cyber Realm reports weekly on cyber-related attacks, trends, hazards and warnings worldwide.
- Open Source Infrastructure Cyber Read File provides a monthly summary of significant cybersecurity and cyber infrastructure incidents, which also include more detailed articles to provide context and sector-specific implications.
- The DHS Daily Open Source Infrastructure Report is directed to infrastructure protection professionals, reporting information pertaining to all infrastructures worldwide.

Senior leaders only invest in what they understand. These information exchanges enable strategic cyber intelligence producers to collect, analyze and disseminate products that are comprehensible and relevant to senior leaders. Information sharing efforts support their strategic decision-making by allowing organizations to better anticipate and respond to cyber threats and to make risk-informed resourcing decisions. Organizations, therefore, must work with internal stakeholders and with their counterparts in government and in peer organizations to share information and analytic products and ensure that information exchange is a two-way relationship.

Strategic insights for risk-informed decision-making

Recall that the DSB Task force defines cyber risk as a function of *threat*, *vulnerability* and *consequences*. Accordingly, the most fundamental elements of risk-informed decision-making in the cyber domain are:

- assessing the value and vulnerability of both tangible and intangible enterprise asset;
- understanding the threats against those assets; and
- aligning investments and countermeasures accordingly.

Asset and vulnerability assessment

Value: Informational assets might include intellectual property, business operations, agency/company financial information and PII. Asset assessment involves appraising value, prioritizing the impact of loss and evaluating those assets' exposure and vulnerability. Strategic cyber intelligence can inform those decisions, but ultimately executive/command level leaders judge value and priority.

Impact: In addition to value, the enterprise should evaluate the potential impacts of a successful exploitation. Impacts are consequences of concern that result in mission or business costs (Ross, 2011a). Cybersecurity seeks to protect informational assets from breach or compromise of confidentiality (through unauthorized disclosure), integrity (through unauthorized modification or destruction) and availability (through unauthorized restriction on access). Negative consequences often arise when one or more of those conditions are compromised. A compromise can create loss (e.g. financial, reputational, competitive advantage) or disrupt business continuity.

Strategic cyber intelligence analyses directly support senior organizational leaders in estimating impacts. Executive/command-level leaders should communicate the impacts they view as critical to the organization's mission or business processes, that is, impacts that disrupt or severely damage operations or that disable business continuity. Senior leadership is ultimately responsible for establishing an organization's strategy, governance and risk tolerance and for developing and executing risk management resourcing strategies, so those top-level personnel should be the primary source for assessing impact/consequence criticality. Strategic cyber intelligence analysis should inform these assessments to reduce uncertainty and improve decision quality.

Assessing the impact of asset loss can be done qualitatively – by heuristic or consensus – or quantitatively using metrics. A commonly used loss metric is the single loss expectancy (SLE). The SLE is a function of the asset's assigned value and the exposure factor. An exposure factor is the subjectively calculated proportion (percentage) of the asset's value that would be lost if a threat exploit against it was successful. For example, if an organization's intellectual property is valued at $1,000,000 and it is estimated that in the event of a breach, 25 per cent of the data could be exfiltrated before detection, then 25 per cent is the exposure factor. Multiplying the value of the asset with the exposure factor yields the SLE, which in this case would be $250,000. The analyst can annualize the loss by estimating how likely that specific exploit, without safeguards, is to occur in a 12-month timeframe. That frequency figure is known as the annual rate of occurrence (ARO).

The SLE when multiplied by the ARO, yields an *annualized loss expectancy* (ALE), which can be used for strategic resource decisions. In this example, assuming that, without safeguards, a successful exploitation is likely to occur once every six months. This equates to an ARO of two (i.e. two events in one year). Therefore, the ALE for this example would be $500,000 ($250,000 $\times$ 2 = $250,000). Using this value as a benchmark, senior leaders know they can spend up to $500,000 per year to mitigate the risk of a data breach and still have the benefits outweigh the costs.

Vulnerability: Strategic cyber intelligence analysis also supports vulnerability-oriented risk analysis. Vulnerability assessments do not describe features of the assets themselves but rather of the assets' exploitability. NIST guidelines advocate for vulnerability-oriented risk analysis to identify:

> […] a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environment in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised (Ross, 2011a).

Vulnerabilities can be technical or contextual, and as the DSB Task Force suggests, can be categorized as either inherent or operationally induced. Cybersecurity professionals often characterize vulnerabilities as weaknesses in people, process and technology (denoted as "PPTs"). Exploitable PPT vulnerabilities exist on a particular plane (often called an "attack surface"). Stephen Northcutt of the SANS Technology Institute recommends that vulnerabilities be assessed on at least three surfaces: network, software and human (Northcutt, 2011).

Across attack surfaces, trust is a key vector for vulnerability[3]. NIST defines trust as "a belief that an entity will behave in a predictable manner in specified circumstances" (Ross, 2011b). NIST further specifies three characteristics commonly associated with trust that it is:

(1) usually relative to a specific circumstance or situation;

(2) generally not transitive; and

(3) generally earned, based on experience or measurement.

Key trust relationships with other organizations and agencies are particular concerns at the strategic level because a risk taken by one is a risk assumed by all. Strategic cyber intelligence analysis should understand and account for these domestic, international, public and private sector linkages and interdependencies, as they develop the model. For example, trust relationships with a particular industry or company size may put an organization at risk.

Threat assessment and alignment

While tactical threat intelligence focuses on bits, code, malware and technical exploits, strategic threat intelligence focuses on actors' intentions, capabilities and tactics, techniques and procedures (TTPs). Strategic cyber intelligence analysis performs estimative analysis to assess the probability or likelihood that a threat agent has the intent and capability to exploit a given vulnerability. Based on the inward-looking inventory of the organization's critical assets, strategic cyber intelligence analysts must then look outwardly to identify and evaluate which cyber threat actors are most likely to target the organization in a cyber incident and why. Understanding both the adversaries of greatest concern and the threat landscape is critical.

Who?: Different threat actors target different kinds of assets. Each enterprise needs to determine which threat vectors pose the greatest risk to its most valued and mission-critical assets. Potential actors of interest may include malicious insiders, cyber criminals, terrorists, hacktivists and nations-states. Especially troublesome are the collaborations and alliances between these different groups (US Government Accountability Office, 2013, pp. 3-4). After identifying the specific threat actor – or category of threat actors – posing the greatest risk of harm, the strategic intelligence analyst can begin profiling the actor/group's motivation and intent, as well as their technical and analytical capabilities.

What?: Another key objective is to discern the types of assets the adversary is most likely to target, including the strategic vulnerabilities they might exploit to compromise the organization's information assets. By assessing these factors, the threat intelligence team provides senior leaders and risk managers with an invaluable tool for understanding the organization's exposure to a potential incident. Cyber threats are dynamic, so this kind of threat analysis is a continuous process.

Why and how?: Strategic intelligence analysts can illuminate the adversary's thought process through the process of "red teaming":

> {R}ed teaming is the practice of viewing a problem from an adversary or competitor's perspective. The goal of most red teams is to enhance decision making, either by specifying the adversary's preferences and strategies or by simply acting as a devil's advocate (Red Team Journal, 2015).

The analytical process should ask, "Based on the adversary's strategic goals, their pattern of TTPs and their ethos, which organizations are they most likely to target and how?" and "What methods are they likely to use to achieve their objectives?" A well-executed red teaming exercise asks these questions through the lens of the adversary's socio-cultural frame of reference, as well as its perspectives of the threat landscape, and perceptions of its constraints, source of authority and its adversary. Red team analysts are well versed in adversary doctrine, strategies, tactics, techniques and procedures. This enables them to "step into the shoes" of the threat actor.

This "know your enemy" exercise has two key benefits. It mitigates the likelihood of "mirror imaging (Heuer, 1999, p. 70)" (assuming the adversary will act as we would act), and it enables the organization to explore an adversary's possible motivation and intent, as well as avenues of attack, including hypothetical scenarios not yet observed in the operating environment. In addition to understanding adversary motivation and intent through red teaming, the threat assessment must also consider how shifts in the threat environment affect adversary behavior and outcomes.

To be clear, strategic threat assessment is not just a snapshot; it is an ongoing process. Cyber threats are dynamic – new techniques evolve, adversaries adapt and changes in the operating environment cause changes in behavior. The snapshot may provide a baseline of an adversary's behavior, but the strategic cyber intelligence analyst must look deeper to discern potential trends and patterns (especially as they pertain to the kinds of targets, TTPs and frequency of attacks), evaluate an adversary's strengths and weaknesses over time and explore key events and situations that may change an adversary's behavioral propensities. This is where a comprehensive understanding of aspects outside of the technical domain is essential to complement the tactical and operational levels cyber intelligence.

Indicators and warnings (I&W) framework: an enterprise-specific framework for I&Ws can provide advanced threat warnings and guide strategic estimates. I&W is a useful tool for discerning meaningful changes in the operating environment. Freyn and Nimalan (2012) have suggested a four-step approach for modifying and structuring the I&W process that can be readily adapted to the cyber domain.

In the first step, the analyst defines the parameters of the target event (or kind of target events) she wishes to forecast and identifies past events that approximate that target threat. The second step requires the analyst to discern key indicators that

preceded those events, especially those that were "necessary" conditions for the exploit. To more systematically identify indicators, Freyn and Paul suggest using a macro-environmental framework such as STEEP (social, technology, economic, environmental, political/legal) to structure the analysis. In the third step, analysts weigh the indicators according to their relevance. Because relevance in I&W analysis is often subjective, Freyn and Nimalan (2012) suggest using an Analysis of Competing Hypotheses methodology to mitigate cognitive bias. The fourth and final step is to develop a quantitative model from weighted indicators. Here, the analyst might assign scores (e.g. 1-4) to each indicator based on its diagnostic value – that is the extent to which it appears specifically to portend a threat. Adding the quantitative scale enables comparisons across different scenarios using a common metric. Methods such as risk scoring of threats and vulnerabilities by potential impact, using business impact analysis and other artifacts can also help align the enterprise's threats, countermeasures and resources.

Focusing on the strategic level, an enterprise might consider the following questions as part of a cyber I&W framework:

(1) How does the enterprise define the threat environment, in terms of mission and business operations?

(2) What is the political and economic landscape in each region of concern? What is the precedent for threat activity in the region? What future outcomes could shift the operating environment?

(3) Can the enterprise mitigate, eliminate, accept, transfer or avoid the risk?

(4) Which threat actors operate in this environment or pose a threat to specific operations?:

- How do these threat actors pose a threat to the enterprise?
- Do the threat actors pose an indirect risk, such as attacks on the enterprise supply chain?
- What factors drive the threat agent's decision-making? What potential changes in the threat environment might impact the adversary's decision tree?
- How do the firm's business operations intersect with the adversary's goals? What changes to the operating environment might increase/decrease the probability of threat activity? What resource decisions will be required to enact those changes?
- What are the threat agent's capabilities; common tactics, techniques and procedures (TTPs); and the likely impacts to the enterprise?

These kinds of questions support an I&W framework that will allow the organization to track current and future threats as they relate to business operations. The organization prioritizes which threat actor classes should be the subject of ongoing intelligence collection. Strategic threat assessment enables organizations to implement defenses and educate stakeholders, giving them a better understanding of an adversary's collection requirements and long-term strategic goals. For example, an energy company may determine that because of its involvement in environmental policy issues, the company is likely to be targeted in any hacktivist campaign focused on global warming.

Therefore, the company integrates collection and analysis of environmental protest activity into its strategic I&W framework.

Regardless of the business context, an effective I&W implementation continually scans the threat environment, and attack surfaces for changes and assesses how the adversary will adapt to changes. Therefore, organizations should supplement strategic I&W collection with an operational I&W program that tracks day-to-day changes in the operating environment.

Conclusion

Nearly every critical system relies on information and communication technology. Cyber risks will continue to proliferate, and organizations in the public and private sectors will act to defend and protect their valued informational assets. Investing in technology, firewalls and intrusion detection systems is appropriate but, by itself, insufficient. As with many other complex security threats, intelligence is a key component. Cyber intelligence emphasizes prevention and anticipation to focus cybersecurity efforts "left of the hack".

Strategic cyber intelligence can substantially reduce risk to the organization's mission and valued assets and support its due diligence. In short, strategic cyber intelligence can focus "intelligence collection and analysis to understand adversarial cyber capabilities, plans and intentions and to enable counterstrategies" (Freyn and Nimalan, 2012, p. 46).

For intelligence to drive the cybersecurity mission, command/executive leaders must be engaged to help identify and develop their CIRs. With those requirements as an azimuth, the cyber intelligence function is positioned to assess the enterprise's threats, vulnerabilities and potential impacts and advise senior leaders on strategic decisions about risk and resourcing. Strategic cyber intelligence analysts can monitor changes in the attack surface and the activity of threat actors who have the intent and capability to exploit the organization's vulnerabilities. Strategic cyber intelligence also adds value to the broader cybersecurity function by:

- enhancing assessment, explanation and quantification of business/mission risks to senior management and other key stakeholders;
- collaborating actively with members of law enforcement, defense and intelligence communities, as well as the sector's information security community;
- demonstrating an appropriate standard of diligence to auditors, regulators and stakeholders, which should reduce business exposure to regulatory or legal sanctions; and
- facilitating responsible expenditure of security resources by aligning asset evaluation with threats, vulnerabilities and enterprise resources to defend not only what is important to the firm but what is relevant to the threat.

Cybersecurity is a team activity with a wide array of stakeholders. Responsibility for strategic cyber intelligence can no longer rest exclusively, or even primarily, with the US federal government. Industries and commercial sectors must collaborate with the government to share and disseminate information, strengthen cyber intelligence capabilities and prevent future cyber incidents.

Notes

1. "information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network […]".
2. See www.americanbar.org/content/dam/aba/marketing/Cybersecurity/2013march21_cyberroleschart.authcheckdam.pdf
3. For an in-depth review of trust, see Borum, Randy. *The Science of Interpersonal Trust.* McLean, Va: The MITRE Corporation/IARPA, 2010.

References

Alexander, K. (2013), "Cybersecurity: preparing for and responding to the enduring threat", *Statement Of General Keith B. Alexander, USA Commander, United States Cyber Command Director, National Security Agency Chief, Central Security Service Before The Senate Committee On Appropriations*, US Senate Committee On Appropriations, Washington, DC.

Borum, R., Felker, J. and Kern, S. (2014), "Cyber intelligence operations: more than just ones and zeroes", *Proceedings of the Marine Safety and Security Council: The US Coast Guard Journal of Safety and Security at Sea, Washington, DC*, Vol. 71 No. 4, pp. 65-68.

Center for Strategic and International Studies (2008), "Securing cyberspace for the 44th Presidency", Center for Strategic and International Studies, Washington, DC, available at: http:csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Central Intelligence Agency (2004), *Conference Report: Intelligence for a New Era in American Foreign Policy*, Central Intelligence Agency, Washington, DC, pp. 3-4.

Dennesen, K., Felker, J., Feyes, T. and Kern, S. (2014), "Strategic cyber intelligence", Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, INSA, Washington, DC.

DoD Defense Science Board (2013), "Resilient military systems and the advanced cyber threat: DSB task force report", Defense Science Board, Washington, DC, available at: www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

Freyn, S. and Nimalan, P. (2012), "Using structured methods to improve indicator and warning analysis", *Competitive Intelligence*, Vol. 15 No. 4, pp. 22-29.

Heidenrich, J. (2008), "The state of strategic intelligence: the intelligence community's neglect of strategic intelligence", *Studies in Intelligence*, Vol. 51 No. 2, available at: www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-state-of-strategic-intelligence.html

Heuer, R. (1999), "Psychology of intelligence analysis", *Central Intelligence Agency*, Center For Study of Intelligence, Washington, DC, available at: www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/

International Multilateral Partnership Against Cyber Threats (IMPACT) (2014), "What we stand for", available at: www.impact-alliance.org/aboutus/mission-&-vision.html

Ludwick, M., McAllister, J., Mellinger, A., Sereno, K. and Townsedn, T. (2013), *Cyber Intelligence Tradecraft Project: Summary of Key Findings*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Mattern, T., Felker, J., Borum, R. and Bamford, G. (2014), "Operational levels of cyber intelligence", *International Journal of Intelligence and Counterintelligence*, Vol. 27 No. 4, pp. 702-719.

National Initiative for Cybersecurity Careers and Studies (NICCS) (2013), *The National Cybersecurity Workforce Framework*, DHS, Washington, DC, available at: http://niccs.us-cert.gov/training/tc/framework/specialty-areas

Noble, R. (2013), "State of the organization address", *82nd INTERPOL General Assembly Session*, Cartagena de Indias, Colombia.

Northcutt, S. (2011), "The attack surface problem", SANS Technology Institute, available at: www.sans.edu/research/security-laboratory/article/did-attack-surface

Office of the Director of National Intelligence (2014), *The National Intelligence Strategy of the United States of America*, Office of the Director of National Intelligence, Washington, DC.

Red Team Journal (2015), "Red teaming and alternative analysis", available at: http://redteamjournal.com/about/red-teaming-and-alternative-analysis/

Ross, R. (2011a), "NIST special publication 800-30", *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology (NIST), Washington, DC.

Ross, R. (2011b), "NIST special publication 800-39", *Managing Information Security Risk Organization, Mission, and Information Systems View*, National Institute of Standards and Technology (NIST), Washington, DC.

RSA (2012), *Getting Ahead of Advanced Threats*, RSA, EMC Corporation, Hopkinton, MA.

Stevens, T. (2013), "Cyberspace and national security: threats, opportunities, and power in a virtual world", *Contemporary Security Policy*, Vol. 34 No. 1, pp. 254-256.

The Ponemon Institute (2013), *The State of Risk-Based Security Management*, Ponemon Institute, Traverse City, MI, available at: www.tripwire.com/ponemon/2013/-metrics

The White House (2009), *Cyberspace Policy Review*, The White House, Washington, DC, available at: www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

US Department of Defense (2011), *Department of Defense Strategy for Operating in Cyberspace*, US Department of Defense, Washington, DC.

US Government Accountability Office (2006), *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, US Government Accountability Office, Washington, DC.

US Government Accountability Office (2013), *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*, US Government Accountability Office, Washington, DC, available at: www.gao.gov/assets/660/652817.pdf

Further reading

The White House (2008), *The Comprehensive National Cybersecurity Initiative*, The White House, Washington, DC, available at: www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

About the authors

Randy Borum is a Professor in the School of Information at the University of South Florida, where he holds a joint appointment the College of Public Health. He has served on the Director of National Intelligence's (DNI's) Intelligence Science Board, the Defense Science Board Task Force on Understanding Human Dynamics and as a behavioral scientist and Board-Certified Forensic Psychologist researching national and global security issues. He regularly teaches and consults with law enforcement agencies, the Intelligence Community and DoD and has authored/co-authored more than 120 professional publications. Randy Borum is the corresponding author and can be contacted at: borum@usf.edu

John Felker is Director, Cyber Intelligence Strategy at Hewlett-Packard Enterprise Services. His primary focus is developing business strategy in DHS, Department of Defense and the Intelligence Community. He recently co-authored "The Operational Levels of Cyber Intelligence" and "The Strategic Level of Cyber Intelligence" for Intelligence and National Security Alliance. In his 30-year Coast Guard career, he commanded several ships, served as a program analyst, led the Coast Guard's International Training Team and stood up both Coast Guard Cryptologic Group as the first commander and Coast Guard Cyber Command as the first Deputy Commander.

Sean Kern, CISSP, is an Adjunct Fellow for Cybersecurity Leadership Policy at the Pell Center for International Relations and Public Policy. He has over 20 years of cybersecurity leadership and management experience in the federal government and co-authored a recent Pell Center report entitled "Professionalizing Cybersecurity: A path to universal standards and status". He is also actively involved with the Intelligence and National Security Alliance Cyber Intelligence Task Force where he co-authored whitepapers on strategic and operational cyber intelligence and the Council on Cybersecurity where he is a contributor to a soon-to-be-released cybersecurity workforce handbook for executives, IT and security managers and HR professionals.

Kristen Dennesen is a Senior Threat Analyst at FireEye Labs. Previously, she managed the Client Directed Research program at iDefense. Her past research initiatives have included geopolitical threat analysis, supply chain risk, strategic red teaming, Mergers & Acquisitions (M&A) cyber risk analysis, strategic indications and warnings (I&W) reports and threat actor capability assessments. She has successfully partnered with numerous Fortune 500 and public sector clients to design research that provides direct decision support to strategic business objectives and risk management functions.

Tonya Feyes is an Intelligence Professional with 24 years of operational experience within the Intelligence Community. Since retiring from a 20-year career in the US Air Force, she has become the President of VHF omnidirectional range (VOR) Technology and the CEO of Task Force (TF) Solutions. She also serves as the Event Manager for the Cyber Security Forum Initiative and as a member of the Cyber Intelligence Task Force for the Intelligence and National Security Alliance. She holds a Bachelor's degree in Intelligence Studies from American Military University and a Master's in Cybersecurity from University of Maryland University College.