2014

Operational Levels of Cyber Intelligence

Troy Mattern
John Felker
Randy Borum
George Bamford

International Journal of Intelligence and CounterIntelligence
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ujic20

Operational Levels of Cyber Intelligence

Troy Mattern , John Felker , Randy Borum & George Bamford
Published online: 06 Aug 2014.

To cite this article: Troy Mattern , John Felker , Randy Borum & George Bamford (2014) Operational Levels of Cyber Intelligence, International Journal of Intelligence and CounterIntelligence, 27:4, 702-719, DOI: 10.1080/08850607.2014.924811

To link to this article: http://dx.doi.org/10.1080/08850607.2014.924811

International Journal of Intelligence and CounterIntelligence, 27: 702–719, 2014

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2014.924811

Routledge
Taylor & Francis Group

TROY MATTERN, JOHN FELKER, RANDY BORUM, and GEORGE BAMFORD

Operational Levels of Cyber Intelligence

The hazards of cybercrime and the challenges of cybersecurity have been widely discussed over the past two decades.[2] In 2012 the security firm Norton reported alarming statistics about the growth of malicious cyber activity.[3]

- In 24 advanced nations there were 556 million victims of cybercrime annually equating to 1.5 million daily or 18 per second[4]

Troy Mattern, Deputy Head of Cyber Security at the Zurich Insurance Company Ltd., is also Chairman of the Cyber Intelligence Task Force of the Intelligence and National Security Alliance (INSA). Previously the European Response Lead at Zurich Insurance, and Technical Director for Cyber Intelligence at the Software Engineering Institute, he is a graduate of the University of Arizona and the American Military University. A retired U.S. Marine Corps intelligence officer, Mr. Mattern has also served as Military Executive Assistant to the Deputy Commander of the United States Cyber Command in the U.S. Department of Defense.

John Felker is Director of Cyber and Intelligence Strategy for Hewlett-Packard (HP) Enterprise Services. His primary focus is developing business strategy in the Department of Homeland Security, the Department of Defense, and the Intelligence Community. He is also co-chair of the Cyber Intelligence Task Force. Previously Vice President for Cyber Security Programs at SCI Consulting, during his thirty-year career with the U.S. Coast Guard, he served as Deputy Commander of the U.S. Coast Guard Cyber Command, and as Commander of the Coast Guard Cryptologic Group. A graduate of Ithaca College, he received his M.A. in Public Administration from the Maxwell School of Citizenship and Public Affairs at Syracuse University.

- Two out of three adults online were victims
- The cost of cybercrime was $110 billion annually, $21 billion in the U.S. alone
- 85 percent of these direct financial costs result from fraud, required repairs or patching, theft and loss of intellectual property

In October 2011, the then-Executive Assistant Director of the Federal Bureau of Investigation, Shawn Henry, reported on a cyber intrusion in which ten years' worth of research and development—valued at $1 billion—was stolen virtually overnight.[5]

Managing these economic and national security hazards in cyberspace has been a vexing problem.[6] Most discourse about cybersecurity solutions has focused on defensive measures, mainly ways to protect the perimeter around

Dr. Randy Borum, Professor and Coordinator of Strategy and Information Analysis in the School of Information at the University of South Florida, previously taught at the Duke University School of Medicine. He has served on the U.S. Director of National Intelligence's Intelligence Science Board, on the Defense Science Board Task Force on Understanding Human Dynamics, and on the National Academy of Science's Steering Committee for Sociocultural Data to Accomplish Department of Defense Missions. He has also worked as a consultant for the U.S. Secret Service. A graduate of James Madison University, with a Ph.D. from the Florida Institute of Technology at Melbourne, Dr. Borum has written extensively on security matters.

George Bamford, Deputy Director of the Border Security Division in the Office of Intelligence and Analysis at the United States Department of Homeland Security, was earlier Chief of its Cyber Threat Analysis Branch. He is also a Commander in the U.S. Coast Guard Reserve, and Team Chief for Operations and Intelligence at the Joint Chiefs of Staff (J-3) National Military Command Center. He was previously a Senior Information Technology Program Manager at the U.S. Department of Defense, and Director of the Acquisition and Program Management Support division of the Transportation Security Administration (TSA). Mr. Bamford is a graduate of the U.S. Coast Guard Academy, with an MBA from the George Washington University School of Business and an MPA from the Harvard University Kennedy School of Government.

This article is adapted, in part, from the Intelligence and National Security Alliance (INSA) White Paper "Operational Levels of Cyber Intelligence," developed by INSA's Cyber Intelligence Task Force in September 2013.[1]

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ujic.

sensitive data, information, and systems. Network and system administrators worry about reacting to network intrusions and compromises so that system downtime is minimized and usage can be continued with minimal interruption. While improving network security and information assurance technology may be necessary, these measures are not sufficient to counter the complex and evolving array of cyber threats. Because current reactive approaches are not working, fundamentally changing how to understand and operate in cyberspace is necessary.[7] A transformed approach to cybersecurity cannot rely solely on responding to known threats; it must also track the capabilities, intentions, and activities of potential adversaries and competitors, as they evolve, in the cyber realm.[8] That set of information and associated functions is referred to as Cyber Intelligence.[9]

Cyber Intelligence seeks to not only understand network operations and activities, but also who is doing them, why, and what might be next. Intelligence functions for cybersecurity include collecting and analyzing information that produces timely reporting, with context and relevance to a supported decisionmaker.[10] Cyber Intelligence is not a collection discipline like signals intelligence (SIGINT) or open source intelligence (OSINT). Instead, similar to "medical intelligence,"[11] it is more of an analytic discipline relying on information collected from traditional intelligence sources intended to inform decisionmakers on issues pertaining to operations at all levels in the cyber domain.

INTELLIGENCE-DRIVEN CYBERSECURITY

Cyber intelligence should drive the cybersecurity mission. Intelligence-led operations require (a) a proactive security posture, (b) a thorough, accurate, timely understanding of the threat environment, and (c) a commitment to decisions based on data. A proactive posture relies on well thought out and dynamic defenses, informed by intelligence, to address both actual and potential threats. Ideally, this approach relies on the full spectrum of an organization's capabilities—from network defense, to public relations, legal efforts, and other business operations. Proactive positioning also relies on a comprehensive and accurate understanding (and in as near real time as possible) of one's own network, and the ability to collect and integrate information sources outside of that network to fully assess the threat environment.

An effective, comprehensive cybersecurity enterprise must look "beyond the network." Too often, discussions about cyber defense or computer network defense tend to focus on only one aspect of the cyber operational spectrum: defensive responses and actions on the network.[12] Similarly, discussions about how to use intelligence in network defense are often limited to network activity itself.

Becoming preoccupied with the details of network activity is easy. That activity is visible and discernible. Reliably *knowing* what is happening on

the network is possible. But cyber threats are not merely a network challenge. 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." Cyber attacks often involve activity that extends beyond a target network, so data collection must go further to capture the relevant pieces. In essence, knowing what isn't known is necessary.

Information sources for cyber intelligence are as broad as for any other intelligence target field. Multiple sources are usually needed to get a complete picture of the threat landscape. Relevant data may come from specific network activity, global cyber activity, organizational policy and action, or from geopolitical events. The data can be open source, proprietary, or classified. What matters most is that it the information is timely, actionable, and relevant, helping to reduce uncertainty for decisionmakers. When analyzed and contextualized, information becomes intelligence. Intelligence is what reduces uncertainty and enables timelier, more cost effective, and more informed decisions about policy, operations, and resource allocation.

THE BEHAVIORAL DIMENSIONS OF CYBER ATTACKS

Network activity is ultimately driven by human behavior.[13] Intelligence provides context to that behavior to facilitate a narrative of an adversary's intent.[14] The existing literature on approaches to threat assessment in other contexts provides some useful guidance for analyzing potential attacks. Threat assessments for targeted attacks are grounded in three fundamental principles:[15]

- An attack is the end result of an understandable and often discernible process of thinking and behavior;
- An attack stems from an interaction among the potential attacker, past events, a current situation, the setting, and the target;
- The key to investigating and resolving threat assessment cases is identifying the "attack-related" behaviors.

These principles can be applied broadly to cyber attacks as well. A cyber attack is, indeed, the end result of a series of actions and events, many of which can be discerned as early warning signals of malicious activity. This is the human dimension that complements the technical data security on which experts currently and almost exclusively rely. Combining behavioral and technical data is what offers a real competitive advantage.[16]

THE PATHWAY TO AN ATTACK

In the field of threat assessment reference is commonly made to the activities in planning and preparing for an attack as "attack related behaviors," and to view those behaviors as steps along a pathway toward an attack.[17] In the field of cybersecurity, one translation of the pathway concept is the "Cyber Kill Chain," an intelligence-driven approach to network defense introduced by Eric Hutchins, Michael Cloppert, and their colleagues from the Lockheed Martin Computer Incident Response Team.[18] A kill chain is a sequence of activities and overall operations that a threat vector must traverse in order to cause an effect. If the sequence can be interrupted or defeated at any point, the threat actor cannot inflict the intended effect. Advanced network defense efforts exploit this kill chain to provide temporal distance between the adversary and the defended network.[19]

The Cyber Kill Chain, as the Lockheed Martin team describes it, begins after the malicious actor has penetrated the defended network long enough to log a discernible pattern of activity. This strategic concept is worthy for a known intrusion, but the principal aim of network defense is to prevent intrusions before they occur.[20] To do this, defenders need to expand their understanding of the attack pathway or kill chain beyond what happens on the network.

A kill chain analysis based on past activity in one's own, or another's, network is very useful. Especially powerful, however, is combining information about network activity with knowledge of potential adversaries, their capabilities, intentions, motivations, and interests—what they might hope to gain from intruding on a targeted network.[21] The decision to conduct a malicious action, the planning required to support it, and the pre-requisite actions needed to create or obtain both capability and access happen neither by automation nor at lightning speed. This implies that references to the "speed of cyber" and the milliseconds necessary for bits of data to traverse the Internet are not the only temporal model to consider, and may not be the best.[22]

Although the actual movement of malicious files and the execution of commands occur at the "speed of cyber," the human-enabled activities necessary to execute malicious cyber operations require planning, preparation, choreographed actions, and an investment of time. Days, weeks, months or even years may be required to: decide to take action; determine objectives; select an avenue of approach to use (through the network, an insider, or the supply chain); collect the required information on what to specifically target; acquire the appropriate capability; develop the appropriate access and then, finally commit the action itself, before assessing the effects and determining if further actions are needed.[23] The time and trail of activity required for that process present opportunities for

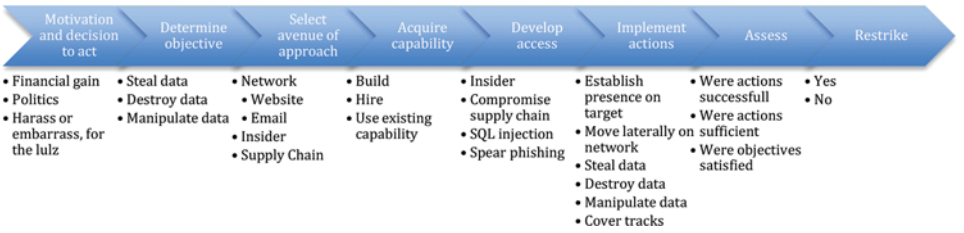

Figure 1. The bulleted examples for each step should be considered as possibilities, not a absolute list of the only options. Cyber intelligence analysts should make assessments as to what are the correct answers for the threats facing them and the missions they are trying to support.

detection and interruption. As malicious actors move along a path from idea to action, or decision to execution (Figure 1), an intelligence-based defense will be sensitive to anomalies, warning signals, and cyber attack-related behaviors.[24]

Recognizing that a series of preparatory steps and actions will precede an attack, intelligence efforts can be deployed to discern:

- who may be targeting a network
- what are the intentions and capabilities of the malicious actors
- when they will conduct their activity
- where the activity will originate
- how they plan to penetrate or affect the network

Malicious cyber actors can have a range of motives and objectives. A nation-state may be trying to steal another government's secrets. A business competitor may try to gain a market advantage. Ideologically motivated hacktivists may try to disrupt an organization that they oppose. Regardless of the motive, each preparatory action presents an opportunity to detect and thwart attacks.[25] When these opportunities are sought out and acted upon, an adversary is pushed into a reactive posture, which can lengthen the time to action and impose additional costs. Just as with physical defenses, the aggressor, upon seeing that the intended victim is a hard target whose defense is agile and adaptive, may choose to look elsewhere.

COMBATING A CYBER ATTACK

The Lockheed Martin intelligence-driven approach to network defense presents a course of action matrix in considering the existing defensive capabilities to detect, deny, disrupt, degrade, deceive, or destroy a malicious actor's efforts target a network (Figure 2). While their examples

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-Line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions of Objectives	Audit log			Quality of Service	Honeypot	

From *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, available at* http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Figure 2. Reactive course of action matrix.

consider only within network actions, the concept can be applied off the network as well. Private companies, governments, and non-governmental organizations (NGOs) have an array of non-network resources available to them. For example, a public relations effort can apply pressure or help modify how the company is perceived. Discussions with a key supply chain vendor may persuade that vendor not to partner with a threat to one's own supply chain. This begins to challenge the notion that the cost of security is prohibitive and that the advantage always lies with the attacker. If the ideas of an intelligence-driven defense are expanded, then friendly actors can use a matrix (Figure 3), tailored towards the user's unique capabilities, to help identify and evaluate options to detect, and then interrupt, malicious actors before they enter the network.

A FRAMEWORK FOR UNDERSTANDING DECISIONS AND CYBER ACTIVITIES

Countering malicious cyber activity is clearly not simply an ''on-the-network'' fight. Cyber Intelligence lies at the confluence of decisionmaking and cyber activity. Both decisions and activities can occur at various levels of operation.[26] A three-part framework often used in both the government and private sector classifies these levels as Strategic, Operational, and Tactical.[27] Though conceptually distinct, in practice the activities at each level often overlap. These definitions help frame the functions and roles appropriate at the various levels, but do not seek to establish an inflexible

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Motivation	Open Source Intelligence	Public Relations, Reputation for prosecuting		Public Relations		
Objectives	Web analytics, Open Source Intelligence			OPSEC	Public Relations	
Avenue of approach	Web/Network analytics		Dynamic Defense	Dynamic Defense, OPSEC	Direct towards stronger defenses	
Capability	Open Source Intelligence		Insider threat program	Dynamic Defense	Direct towards stronger defenses	
Access	Open Source Intelligence, web/network analytics	Insider threat program		Dynamic Defense, OPSEC		
Actions	Insider threat program, Supply chain awareness, Intel-driven CND	Role based access		Quality of Service	Honeypot	
Assess	Web analytics, Social Media	Public Relations			Public Relations, Honeypot	
Restrike	Web/Network analytics, Open Source Intelligence,	Dynamic Defense			Public Relations, Honeypot	

*Organization Chief Information Security Officers (CISCOs) and Chief Information Officers (CIOs) should consider their own operational environment as well as what resources their organizations have in order to fill in the matrix so it is accurate and useful for their purposes.

Figure 3. Proactive course of action matrix.

structure that is too rigid to meet real world mission requirements or operational realities.

The Strategic Level of Cyber

The strategic level of planning and control focuses on establishing an organization's mission and direction, setting objectives, and developing a plan for how those objectives will be achieved. The Department of Defense defines the Strategic level as:

> The level . . . at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic

> security objectives and guidance, and develops and uses national resources to achieve these objectives [emphasis added].

Accordingly, the strategic level of cyber activity pertains to an organization's general direction, specific goals, and resource allocation in service of its mission, as guided by the highest-level executive or command entity. A consideration of "what do we have that others want," "how valuable/important is it," and "how well are we protecting it" begins the process of risk assessment. Leadership must answer these questions in its assessment of asset risk, vulnerability, and value. The threat landscape should then be assessed to discern what the invaders want to achieve, and how they will likely attempt to achieve those aims.

Such adversary activity might include:

- The decision to use cyber capabilities to acquire information or technology;
- The decision to attack a particularly sensitive or strategically important target;
- The action of allocating resources towards developing general capabilities for exploitation or attack.

Executive and policy-level decisionmakers must have access to accurate, relevant, and timely intelligence to help them understand the threats that may hinder the organization's pursuit of its strategic objectives. In the United States government, strategic decisionmakers include the President and the National Security Staff. This category may extend to the senior and command levels of the Departments of Defense, Justice, and Homeland Security, as well as Cabinet principals. In the corporate world, strategic decisions are principally in the purview of the chief executive officer, the chief operations officer, the chief financial officer, executive management teams, and corporate boards because these individuals establish overarching corporate objectives, policies, priorities, and ultimately allocate the resources. Chief information officers (CIOs) and chief information security officers (CISOs) do not typically fall into the category of strategic decisionmakers. While they are critically important to the security and functioning of the networks, most corporate and government environments do not afford CIOs and CISOs the ability to establish broad objectives for the corporate enterprise.

Intelligence is typically considered to have strategic importance if it reveals new or changed risk pertinent to the organization's overarching mission. Some examples might include:

- The decision by a competitor or potential competitor to enter a firm's market space (e.g., a foreign competitor's new five-year plan now shows interest in developing a domestic capability in a technology the target company is known for);

- Indications that a competitor, or foreign government, may have previously acquired intellectual property via cyber exploitation;
- Indications that a competitor, or foreign government, is establishing an atypical influential relationship with a portion of the target's supply chain;
- Indications that a firm's corporate strategic objectives may be threatened due to adversarial cyber activity.

Some network security professionals might not readily see the value of this information because they would probably not regard it as actionable. But this information matters because it will help influence senior executive decisionmaking on (1) corporate strategic objectives, (2) the appropriate priority of cyber security/intelligence support, and (3) the appropriate allocation of resources towards the security mission vis-à-vis the threats and other operational priorities. A return-on-investment decision is being made at the corporate level. Without this information, a chief executive may prioritize and allocate resources to other mission functions that appear to more directly and tangibly contribute to the organization's strategic objectives. Consequently, funding decisions for cybersecurity may be based on inadequate appraisals of the threat environment and the implications of those threats for mission assurance.

The Operational Level of Cyber

The operational level of planning and control focuses on enabling and sustaining day-to-day operations and output, including logistics. The Department of Defense defines the operational level as:

> The level . . . at which *campaigns and major operations are planned, conducted, and sustained* to achieve strategic objectives within theaters or other operational areas [emphasis added].

Cyber intelligence, at this level, involves tracking how malicious forces plan and prepare their attacks based upon what they have learned in collecting their own intelligence and on what they deem necessary based upon their strategic goals. Attackers must build the infrastructure (e.g., botnets, malware, delivery methodology, such as phishing) needed to support their tactical operations. They maneuver in cyberspace (hop points) to position their capabilities where needed to execute their tactics. At the operational level, a hacktivist group, for example, may plan both cyber and physical world activities to support their objectives.

Some examples of operational level intelligence include:

- Trend analysis indicating the technical direction in which an adversary's capabilities are evolving.

- Indications that an adversary has selected an avenue of approach for targeting an organization.
- Indications that an adversary is building capacity to exploit a particular avenue of approach.
- The revelation of adversary tactics, techniques, and procedures.
- Understanding the adversary's operational cycle (i.e., decisionmaking, acquisitions, command and control (C2) methods for both the technology and the personnel).
- An adversary's technical, social, legal, financial or other vulnerabilities.
- Information that enables the defender to influence adversaries as they move along a pathway (through the kill chain) to their attack.

Operational-level planning for security operations and campaigns falls mainly to the CIO and the CISO. Their responsibility is to plan appropriate support for new endeavors, temporary or otherwise. They also have the responsibility to allocate and maintain operational information technology systems and security support to ensure that their organization can achieve its objectives and accomplish its mission. Similarly, they must not only track malware that has penetrated their systems, but also understand who is doing it, why, and what their capabilities are, so they can stay ahead of the attacks. Operational-level controls afford opportunities to design intelligence-based defenses against known and likely threats to an organization's network and data. That is, they facilitate knowledge of who and what the threats are before they are inside the wire. The more that CISOs and CIOs can learn about the objectives of malicious actors, and what is within their capability, the better able they will be to posture their enterprise to defend against them, thwart their actions, and be more resilient.

The Tactical Level of Cyber

The tactical level of planning and control focuses on the specific steps and actions taken to enact a strategy. The U.S. Department of Defense defines the tactical level as:

> The level . . . at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. Activities at this level focus on the *ordered arrangement and maneuver of combat elements in relation to each other and to the enemy* to achieve combat objectives [emphasis added].

In the cyber domain, the tactical level is where on-the-network actions take place. This is where malicious aggressors and network defenders maneuver actively against each other. Botnets may be directed toward a specified target and unleash their payloads. An adversary finds vulnerabilities and infiltrates a network. An aggressor using advanced persistent threats maneuvers

laterally inside the target network, seeking the wanted information, copies it, encrypts it and exfiltrates the data. The tactical level is where most of the cyber defense attention is focused today. While the tactical level is important, focusing exclusively on tactics means that the adversary is either in the network already, or at the door of the gateway trying to get in. But if appropriate resources had been expended at the previous two levels some of an adversary's tactical activity might have been prevented.[28]

Tactical defenses are executed primarily in an organization's Network Operations or Security Operations Center and may include: host-based security system alerts, signature or behavior detection efforts, and in advanced cases, the use of pathway/kill chain analysis based on assessments of known forces or network behavioral patterns. The tactical level, as with the operational and strategic levels, operates best when driven by intelligence.

Consider, for example, a Network Operations Center that not only anticipates being targeted for a distributed denial of service (DDOS) attack, but can discern a high-risk time window for the attack. This information is often knowable, particularly because some hacktivists make little effort to conceal when they intend to strike. Others openly advertise the fact they intend to do so. By integrating analyses of geopolitical events, assessing the likelihood and timeframe of an attack is often possible.[29] With intelligence regarding the "time window," defenders could coordinate in advance with their Internet Service Provider (ISP) and surge support to re-route incoming traffic from high-demand request points. Armed with that information, the ISP could potentially help identify and shut down the attacker's command and control nodes, which could limit the severity and impact of the DDOS attack. This type of pre-coordination and advanced warning may alone make the difference between critical Web support services being available or not, even if the attack is not thwarted completely.

ALIGNING THREATS AND DEFENSES

Provided here are two examples of conceptual frameworks that could support an intelligence-driven cybersecurity enterprise. First, is the Cyber Prep framework, which proposes a set of escalating threat levels and associated defenses, then comes the Early Warning framework, designed specifically to track and contextualize politically motivated cyber attacks.

Taking the three levels of operational control a step further, Deborah Bodeau and her colleagues, Richard Graubart and Jennifer Fabius-Greene, from The MITRE Corporation created a matrix, aligning levels of cyber preparedness (which they call "Cyber Prep") with levels of threat.[30] They

propose five Cyber Threat Levels, each of which corresponds to a general strategy/posture of cyber defense designed to support mission assurance:

- Threat Level 1: Cyber Vandalism, which corresponds to Perimeter Defense
- Threat Level 2: Cyber Theft/Crime, which corresponds to a defense approach of Critical Information Protection
- Threat Level 3: Cyber Incursion/Surveillance, which corresponds to a defense approach of Responsive Awareness
- Threat Level 4: Cyber Sabotage/Espionage, which corresponds to a defense approach of Architectural Resilience
- Threat Level 5: Cyber Conflict/Warfare, which corresponds to a defense approach of Pervasive Agility

Within each Threat Level, the Bodeau group described how the organization is likely to view the threat (organizational perspective), the purpose of its countermeasures (organizational goals), the organization's overarching plan/strategy for countering the threat (organizational strategy), the typical threats forces (e.g., hackers, nation-state) and the typical intent of those attackers (e.g., disruption/embarrassment of the victim organization, obtain/modify specific information). They also provide scenarios representing each level; examples of tactics, techniques, and procedures that adversaries might use (e.g., defacing files on publicly accessible systems, inserting counterfeited hardware into the supply chain); and examples of possible security measures and solutions (e.g., perimeter firewalls, partitioning internal information infrastructure into subnetworks).

The Cyber Prep framework acknowledges that different organizations at the same threat level may require substantially different solutions. The most effective defense for a given organization will depend on the threat environment and enterprise architecture. The organization should use accurate, timely cyber intelligence, to identify the TTPs most likely to be deployed against them, the vulnerabilities of their own assets, and the potential impact of penetration and compromise. The Cyber Prep framework offers one model for harmonizing and integrating cyber intelligence across the strategic, operational, and tactical levels.

Another framework for understanding and framing the cyber attack process is Ned Moran's Early Warning Model.[31] Moving beyond a general framework for enterprise cyber defense, Moran has outlined a model that specifically describes politically motivated cyber attacks. His early warning model comprises a linear five-stage pathway, which begins with latent tensions between nations or political adversaries and culminates in a cyber attack.

While the Cyber Prep framework presents a hierarchical set of threat levels that may come from different threat vectors, levels in the Early Warning

model represent escalation or forward motion toward a given attack from an identified or identifiable vector in the context of a political conflict or competition, particularly at the nation-state level.

Moran's stages of a politically motivated cyber attack are as follows:

- *Latent Tensions*: This level characterizes the unexacerbated grievances and hostilities that exist (and often persist) between political entities.
- *Cyber Reconnaissance*: This level corresponds to a political entity's attempts to probe, and possibly test for vulnerabilities, in another entity's cyber infrastructure.
- *Initiating Event*: This level marks a "flare up" in the inter-party tensions, which elevates hostilities and perceptions of threat.
- *Cyber Mobilization*: This is the level at which a political entity manipulates the narrative of the "initiating event" to incite action against the other entity.
- *Cyber Attack*: This level represents one entity's attack on the other's cyber infrastructure, often using intelligence gained from its reconnaissance.

Instead of proposing specific cyber defense tactics for each level, in the Early Warning Model, each stage corresponds to a specified Defensive Readiness Condition (DEFCON) for cyberspace. Like the DEFCON system used for military readiness, the levels range from DEFCON 5 for Latent Tension (normal state of readiness), up to DEFCON 1 (imminent threat) for the Cyber Attack. Although the Early Warning Model was developed for politically motivated attacks, the concept could be easily adapted to a range of competitive situations, including those involving business adversaries.

UNDERSTANDING POTENTIAL CYBER VULNERABILITY

Cyber defense is a complex, as yet undefined, multifaceted approach to framing, thinking about, and reacting to adversarial cyber activity. Many discussions emphasize the complexity of the cyber operational domain, the speed with which activity and operations take place, and the supposed inherent advantage of the attacker. By beginning to define the threat environment and the problem set in manageable operational levels, emphasizing the importance of integrating sound and time-tested intelligence thinking and methodology into the equation, it will simplify the problem. This methodology makes possible a better understanding and anticipation of an adversary's actions and intent, thereby providing more accurate, relevant, and timely intelligence for each level of operation.

Understanding, even at a basic level, the cyber "lay of the land" should also help illustrate the need for cyber intelligence analysts to know, and seek to know, far more than just network activity and functionality. To understand how to support operational level requirements, cyber intelligence analysts

need to understand the human dimension of the threat: what malicious actors intend, how they plan, coordinate, and execute, as well as what motivates them towards action or inaction. To support their organizations' strategic goals, analysts likely need to understand the intricacies of current and past geopolitical events, the competitive business landscape, international politics or, in some cases, domestic politics and the agendas of niche interest groups.

As with protecting a home or business from theft or destruction, cybersecurity begins with understanding the criminal or adversary, their intentions, their methodologies, and their opportunity. Whether attacks are initiated by local or transnational criminal forces, a business competitor, a nation–state, or a criminal organization, knowing and understanding its operational/business environment, its own exposure (threats and vulnerabilities), and having a clear sense of what is most valuable (and worthy of expense in time effort and money) within its own network, are critical factors for focusing limited resources, analyzing key risks, and determining the optimal path an organization will forge to achieve its business or mission objectives. Intelligence is leveraged to reduce uncertainty for the decisionmaker and to prevent surprise events, including crime, disruption, or attack. Clearly, more decisionmakers are involved than those in a singular network operations center. The challenge now is to enable decisionmakers, at all levels, to fully understand what information is needed and how to work with a cyber intelligence service or team to collect, integrate, and make that data accessible and actionable to those who must act on it to deter, thwart, or limit malicious network activity.

REFERENCES

[1] George Bamford, John Felker, and Troy Mattern, "Operational Levels of Cyber Intelligence," Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2013.

[2] Han-Chieh Chao, Sherali Zeadally, and Gregorio Martinez, "Securing Cyberspace in the 21st Century," *Computer,* Vol. 46, No. 4, 2013, pp. 22–23; Paul Marks, "Cybersecurity Guru: Hunt for the Next Generation of Hackers," *New Scientist,* Vol. 213, No. 2854, 2012, p. 29; Efstratios Gavas, Nasir Memon, and Douglas Britton, "Winning Cybersecurity One Challenge at a Time," *Security & Privacy, IEEE*, Vol. 10, No. 4, 2012, pp. 75–79. Kim Andreasson, ed., *Cybersecurity: Public Sector Threats and Responses*, Vol. 165. CRC Press, 2012; Steven R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line," *Journal of National Security Law and Policy*, No. 4, 2010, p. 27. Tim Stevens, "Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World," *Contemporary Security Policy,* Vol. 34, No. 1, 2013, pp. 254–256.

[3] Norton Company, "Norton Cyber Crime Report," 5 September 2012, at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[4] The Norton study sample included Australia, Brazil, Canada, China, Colombia, Denmark, France, Germany, India, Italy, Japan, Mexico, Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, South Africa, Sweden, Turkey, United Arab Emirates, United Kingdom, and the United States of America.

[5] Shawn Henry, speech of 20 October 2011 at the Information Systems Security Association International Conference, Baltimore, MD, at http://www.fbi.gov/news/speeches/responding-to-the-cyber-threat

[6] Eloise F. Malone and Michael J. Malone, "The 'Wicked Problem' of Cybersecurity Policy: Analysis of United States and Canadian Policy Response," *Canadian Foreign Policy Journal*, Vol. 19, No. 2, 2013, pp. 158–177.

[7] James A. Lewis, "Raising the Bar for Cybersecurity," Center for Strategic and International Studies, Washington, DC, 2013.

[8] Melissa Ludwick, Jay McAllister, Andrew D. Mellinger, Kathryn Ambrose Sereno, and Troy Townsend, "Cyber Intelligence Tradecraft Project: Summary of Key Findings," Software Engineering Institute, Carnegie Mellon University, 2013.

[9] Barbara Fast, Michael Johnson, and Dick Schaeffer, "Cyber Intelligence: Setting the Landscape for an Emerging Discipline," Cyber Intelligence Task Force, Intelligence and National Security Alliance (INSA) White Paper, 2011.

[10] Matthew M. Hurley, *For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance*, Air University Maxwell Air Force Base, AL, Air Force Research Institute, 2012.

[11] U.S. Defense Intelligence Agency, public affairs press release, "U.S. Dedicates National Center for Medical Intelligence; Pentagon Facility Expands into National Mission," 2 July 2008, at Defense Intelligence Agency website: http://www.dia.mil/public-affairs/releases/2008-07-02.html

[12] Daojing He, Sammy Chan, and Yan Zhang, "How Effective are the Prevailing Attack-defense Models for Cyber Security Anyway?" 2013, pp. 1–1, at http://ieeexplore.ieee.org/iel7/9670/5196652/06636288.pdf?arnumber=6636288, accessed 11 November 2013.

[13] Si Li, Ryan Rickert, and Amy Sliva, "Risk-Based Models of Attacker Behavior in Cybersecurity," in *Social Computing, Behavioral-Cultural Modeling and Prediction*, (Berlin/Heidelberg: Springer, 2013), pp. 523–532.

[14] Gina F. Thomas, Samuel R. Kuper, Krystal M. Thomas, Erik W. Armbrust, and Michael W. Haas, *Understanding the User can be a Tool for Cyber Defense*. No. AFRL-RH-WP-TP-2012–0031; Air Force Research Lab Wright-Patterson AFB, OH Human Performance Wing (711th) Human Effectiveness Directorate/Warfighter Interface Division, 2012. See also Martin C. Libicki, *Brandishing Cyberattack Capabilities*, (Santa Monica, CA: RAND Corporation, 2013), at http://www.rand.org/pubs/research_reports/RR175

[15] Randy Borum, Robert Fein, Bryan Vossekuil, and John Berglund, ''Threat Assessment: Defining an Approach to Assessing Risk for Targeted Violence,'' *Behavioral Sciences & the Law*, Vol. 17, 1999, p. 329. Robert A. Fein and Bryan Vossekuil, ''Protective Intelligence & Threat Assessment Investigations,'' *NIJ Publication* 170612 (1998).

[16] Yang Wang, ''Cybersecurity Research Collaboration Between Computer Scientists and Social Scientists,'' *Social Science, Computer Science, and Cybersecurity Workshop Summary Report*, 2013, p. 28. Klaus Julisch, ''Understanding and Overcoming Cyber Security Anti-Patterns,'' *Computer Networks*, Vol. 57, No. 10, 2013, pp. 2206–2211. Jens Grossklags,''Towards Effective Behavioral and Economic Security Engineering,'' *Social Science, Computer Science, and Cybersecurity Workshop Summary Report*, 2013, p. 20.

[17] Randy Borum, Robert Fein, Bryan Vossekuil, and John Berglund, ''Threat Assessment: Defining an Approach to Assessing Risk for Targeted Violence,'' p. 329.

[18] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, ''Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,'' in *Leading Issues in Information Warfare & Security Research*, No. 1, 2011, p. 80.

[19] Charles Croom, ''The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy,'' *High Frontier: The Journal for Space and Cyberspace Professionals*, Vol. 6, No. 4, 2010.

[20] Newton Lee, ''Cyber Attacks, Prevention, and Countermeasures,'' in *Counterterrorism and Cybersecurity* (New York: Springer, 2013), pp. 119–142.

[21] Klaus Julisch, ''Understanding and Overcoming Cyber Security Anti-Patterns,'' pp. 2206–2211.

[22] So Jeong Kim and Soonjwa Hong, ''Study on the Development of Early Warning Model for Cyber Attack,'' in *Information Science and Applications (ICISA), 2011 International Conference on IEEE*, 2011, pp. 1–8.

[23] Gregory Rattray and Jason Healey, ''Categorizing and Understanding Offensive Cyber Capabilities and Their Use,'' in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy*, No. S 23, 2010.

[24] Ned Moran, ''A Cyber Early Warning Model,'' in *Inside Cyber Warfare: Mapping the Cyber Underworld*, Jeffey Carr, ed. (O'Reilly, 2010), pp. 180–188. Song Chen and Vandana P. Janeja, ''Human Perspective to Anomaly Detection for Cybersecurity,'' *Journal of Intelligent Information Systems*, 2013, pp. 1–21.

[25] Keshav Dev Gupta and Jitendra Joshi, ''Methodological and Operational deliberations in Cyber Attack and Cyber Exploitation,'' *International Journal*, Vol. 2, No. 11, 2012.

[26] Patrick Brézillon and Jean-Charles Pomerol, ''Framing Decision Making at Two Levels,'' in Ana Respício, Frederic Adam, Gloria Phillips-Wren, Carlos Teixeira, and Joao Telhada, eds., *Bridging the Socio-Technical Gap in Decision Support Systems: Challenges for the Next Decade*. Vol. 212 (Amsterdam: IOS Press,

2010), pp. 358–368. Katherine Hibbs Pherson and Randolph H. Pherson, *Critical Thinking for Strategic Intelligence* (Thousand Oaks, CA: Sage, 2012).

[27] For simplicity, we have chosen to use the current Department of Defense definition of these terms from the Dictionary of Military and Associated Terms,[38] Joint Publication 1-02, at http://www.dtic.mil/doctrine/dod_dictionary/). Ramon Casadesus-Masanell and Joan Enric Ricart, "From Strategy to Business Models and onto Tactics," *Long Range Planning*, Vol. 43, No. 2, 2010, pp. 195–215.

[28] The Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force will seek to demonstrate this in future white papers.

[29] Ned Moran, "A Cyber Early Warning Model," pp. 180–188.

[30] Deborah J. Bodeau, Richard Graubart, and Jennifer Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels," *Social Computing (SocialCom), Second International Conference on IEEE*, 2010, pp. 1147–1152.

[31] Ned Moran, "A Cyber Early Warning Model," pp. 180–188.