



OPERATIONAL CYBER INTELLIGENCE

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

INSA CYBER INTELLIGENCE TASK FORCE

OCTOBER 2014



ACKNOWLEDGEMENTS

INSA CHAIRMAN

Ambassador John Negroponte

INSA SENIOR INTELLIGENCE ADVISOR

The Honorable Charlie Allen

INSA SENIOR NATIONAL SECURITY ADVISOR

Ambassador Bob Joseph

INSA STAFF

Ambassador Joe DeTrani, *President*

Chuck Alsup, *Vice President for Policy*

Maureen McGovern, *Senior Fellow*

Ryan Pretzer, *Policy and Public Relations Manager*

English Edwards, *Communications & Marketing Coordinator*

Will Cullin, *Intern*

Rick Dembinski, *Intern*

Adam Goldwater, *Intern*

Noel Hardesty, *Intern*

Garrett Johnson, *Intern*

INSA CYBER COUNCIL CO-CHAIRS

Terry Roberts, *Vice President for Cyber Engineering & Analytics* **TASC**

Ned Deets, *Director, Software Solutions Division*



CYBER INTELLIGENCE TASK FORCE WRITING TEAM

Steven Hengel Jr., *Cyber Threat Intelligence Analyst*

Sean Kern, *Lt Col, USAF, Assistant Professor, National Defense University iCollege*

Andrea Little Limbago, *Principal Social Scientist* **ENDGAME.**

CYBER INTELLIGENCE TASK FORCE EDITING TEAM

John Cassidy, *Branch Director*  CenturyLink

David J. Di Tallo, *CDR, USN, Military Faculty, National Defense University iCollege*

John Felker, *Director, Cyber Intelligence Strategy* 

John Phillips, *Security Researcher*  KEYW

Charlie Shaw, *President, Charles E. Shaw Technology Consulting, Inc.*

EDITORIAL REVIEW

Joe Mazzafrro 

Participation on the Task Force/Council or Subcommittee does not imply personal or official endorsement of the views in the paper by any members or their respective parent organization(s).

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.



EXECUTIVE SUMMARY

In the September 2013 white paper, *The Operational Levels of Cyber Intelligence*, the Intelligence and National Security Alliance (INSA) proposed definitions for the strategic, operational, and tactical levels of cyber activity. While there has been much emphasis on tactical cyber intelligence to help understand the “on the network” cyber attacks so frequently in the news, there has been little discussion about the strategic and operational levels in order to better understand the overall goals, objectives, and interrelationships associated with these tactical attacks. As a result, key consumers such as C-suite executives, executive managers, and other senior leaders in the public, private, and academic sectors are not getting the right type of cyber intelligence to efficiently and effectively inform their organizations’ risk management programs. This traditionally tactical focus also hampers the ability of the cyber intelligence function to communicate cyber risks in a way that leaders can fully interpret and understand.

With cyberspace operating in nanoseconds, the importance of defenses to cyber threat vectors identified by operational cyber intelligence becomes apparent. The fundamental purpose of this white paper is to promote thought and dialogue on the importance of operational cyber intelligence to senior leaders’ risk-informed decision making, which will ultimately lead to improved strategy-based plans and policies to protect their organization against potential adversaries. This paper discusses:

- Operational cyber intelligence and how it seeks to protect the enterprise by facilitating predictive analysis and a more comprehensive understanding of specific threats;
- Business and mission considerations for operational cyber intelligence; and
- Workforce and skill sets necessary to support the cyber intelligence role.

Operational cyber intelligence bridges the broad, nontechnical nature of strategic cyber intelligence and the narrow, technical nature of tactical intelligence. It serves the organization’s executive and functional managers. It informs the development of organizational plans and policies that will direct the organization’s operations over the near term.

The ultimate goal of such a cyber intelligence program is to reduce risk to an organization’s critical mission and assets. Operational cyber intelligence does this by:

- Defining the operating environment;
- Describing the impact of the operating environment;
- Evaluating the adversary; and
- Determining potential adversarial courses of action (COA).

In short, operational cyber intelligence provides a thread that links the probability and impact of a cyber attack with its strategic level implications by providing a coherent framework for analysis and prioritization of potential threats and vulnerabilities given the organization’s threat environment.

OPERATIONAL CYBER INTELLIGENCE

Operational cyber intelligence bridges the broad, nontechnical nature of strategic cyber intelligence and the narrow, technical nature of tactical intelligence. Strategic cyber intelligence, as described in *Operational Levels of Cyber Intelligence*, enables senior decision makers to make more informed decisions regarding resource allocations to achieve an organization's strategic objectives.¹ Operational cyber intelligence serves the organization's executive managers in developing strategy-based plans and policies to protect the organization against potential adversaries. While tactical cyber intelligence is directed at efforts to detect and respond to adversaries already operating within the organization's network, operational cyber intelligence protects the enterprise by facilitating predictive analysis of specific threat actors *before* they gain access to an organization's network.

Strategic and operational cyber intelligence differ in their scope of inquiry. The strategic level assesses risk from a broad worldview, while the operational level focuses on an organization's immediate operating environment. The INSA Cyber Intelligence Task Force has adopted the process presented in Joint Publication 2-01.3, Joint Intelligence Preparation of the Operational Environment (JIPOE), as the general organizing framework for this white paper.² The focus of this white paper is on operational cyber intelligence and its relationships with the strategic and tactical levels of cyber intelligence. In the March 2014 INSA white paper, *Strategic Cyber Intelligence*, the Task Force listed six criteria to describe the levels of cyber intelligence:

1. The nature, role, and identity of the consumer;
2. The decisions the consumer will make;
3. The time frame in which the consumer tends to operate;
4. The scope of collection;
5. The characterization of potential adversaries; and
6. The level of technical aptitude available for cyber intelligence collection.³

Operational cyber intelligence bridges the broad, nontechnical nature of strategic cyber intelligence and the narrow, technical nature of tactical intelligence.

Applying these criteria, operational cyber intelligence is produced for executive management, business unit managers, and contemporaries in both private and public sectors. It focuses on intrasector trend analysis, adversaries' stated and unstated interests, and other operational indications and warnings (I&W). It is used to inform organizational plans and policies that will direct near-term operations. The exact planning horizon varies for each organization, but the time frame enables the organization to proactively implement plans and policies to mitigate risk. Collection will primarily target cyber intelligence related to the organization's sector.

Adversaries of interest may include nations, non-state actors, and individuals with intent and capability.

This white paper will discuss:

- How operational cyber intelligence supports an assessment of the operational environment;
- How operational cyber intelligence is engaged to forecast and assess an adversary's courses of action (COA); and
- How an operational cyber intelligence workforce should be developed.

OPERATIONAL CYBER INTELLIGENCE & THE OPERATING ENVIRONMENT

Operational cyber intelligence continuously assesses the organization's operating environment, helping intelligence analysts identify I&W of potential cyber risks. These indicators relate to the conditions, circumstances, and influences that affect the organization's critical mission and business functions and bear on the decisions of leadership. Operational cyber intelligence analysts must take a holistic perspective when assessing indicators such as intelligence gathering techniques of the adversary, the cyber maturity level and the technical, social, legal, financial or other vulnerabilities of the adversary, ensuring that they account for complex interaction of friendly, adversarial, and neutral systems. These systems may be influenced by political, economic, social, infrastructure, or other relevant aspects of the operating environment. Ultimately, this process results in an assessment of specific adversarial technical and analytical capabilities and their intentions in terms of the most common, most likely, and most dangerous threat vectors they may employ.

Assessing intent and capabilities can be a daunting task because the adversary is intelligent and constantly adapting as organizations implement new countermeasures. Known as threat shifting, the adversary may add additional resources, change its targeting or timing, and adopt new tactics, techniques, and procedures (TTPs) in order to achieve its objectives. Through predictive analysis, operational cyber intelligence assesses the manner in which the adversary is likely to adapt. This intelligence is then used to update organizational plans and policies.

Operational cyber intelligence involves four steps:

1. Define the operating environment;
2. Describe the impact of the operating environment;
3. Evaluate the adversary; and
4. Determine adversarial COA.

DEFINE THE OPERATING ENVIRONMENT

The operating environment includes the range of adversarial actors as well as the range of socioeconomic, political, and military trends that can impact an organization. This step assists the organization in bounding the problem space and identifying areas for further analysis. Defining the operating environment helps identify potential adversaries and the level of risk each adversary represents, identify an organization's vulnerability to malicious behavior in a dynamic global environment, and bridge strategic and operational level analyses.

At the operational level, an organization's operating environment can be described in terms of physical, logical, information, and social layers.⁴ The physical layer refers to the actual information infrastructure - including sensors, servers, and supercomputers - and is grounded in a specific geographic location, which further implies specific authorities and jurisdictions that may influence operations. The logical layer represents a series of platforms and services on which new capabilities are built, enabling information flow. The information layer includes the creation, processing, and storage of the vast range of data on the network - from internal, sensitive communications to systems' configurations to trade secrets and intellectual property.⁵ All cyber activity eventually can be traced back to human actions or social behavior. Therefore, cyber activity is ultimately the result of human motivation, behavior, and intent. The social layer entails a concerted understanding of human behavior at the group level regarding how the groups are influenced by their surroundings and their access to and willingness to employ malicious cyber measures.

An organization's place in the operating environment also includes the geopolitical, cultural, economic, information, and infrastructure aspects of the global system. Organizations linked to certain ethnic, religious, or national affiliations may be more at risk of attack by groups that have historical conflicts with them. While some organizations are more at risk due to the geopolitical landscape - such as the Syrian Electronic Army's alleged attack on the *New York Times* or the attacks on Google within China - much of cyber behavior is simply driven by incentives and lacks ideological or cultural undertones. In this context, it is equally important for organizations to understand where they fit within a given sector, supply chain, and geostrategic location in order to help identify the range of potential adversaries and how they are likely to act.

While it may seem that only big businesses and governments should be concerned, Verizon reported in 2012 that 71 percent of reported data breaches occurred in organizations with fewer than 100 employees.⁶ Relationships with suppliers, partners, customers, and competitors are critical factors to consider in an organization's operating environment. A recent Mandiant report described how a global energy company wanted to assess whether their larger information technology (IT) ecosystem had been compromised. The study found that two of the organizations had been compromised in order to obtain access to the third company.⁷ A systems view of an organization's ecosystem can illuminate the operating environment. This could be particularly relevant when assessing cybersecurity risks related to acquisition, mergers, or any trusted network relationship.

Finally, the operational environment is extraordinarily dynamic, especially in the current era. An organization's risk could follow temporal patterns, such as a greater seasonal risk around the holidays as exhibited by the attack on Target, or it could follow global events such as elections. Therefore, organizations should frequently assess their operating environments to remain aware of

“All cyber activity eventually can be traced back to human actions or social behavior. Therefore, cyber activity is ultimately the result of human motivation, behavior, and intent.”

changes. Maintaining knowledge and understanding of the situation, executive management, business unit managers, and equivalents can compile operational risk assessments and inform COA and cyber defense decisions for decision makers.

EXAMPLE

Pro-Ukrainian media outlets are covering protests related to the Ukrainian president's position on alignment. Pro-Ukrainian protesters seek alignment with NATO and the EU. Pro-Russian Ukrainians seek alignment with Vladimir Putin and Russia. Pro-Ukrainian media outlets want to ensure that they can continue to report the news to internal as well as external audiences. Denials of service, website defacement, and false reporting are very real concerns. The media outlets are fully aware of the precedent Russia has set in previous conflicts with Estonia and Georgia regarding the employment of cyber means to deny, degrade, disrupt, and deceive. There may also be other actors, both internal and external to Ukraine that are Pro-Russian and have the intent and capabilities to affect Pro-Ukrainian media operations. Although early attacks will be perpetrated by proxies, as the stakes get higher, Russia may use state-sponsored means as well. The trigger for this could be the deployment of Russian troops.

DESCRIBE THE IMPACT OF THE OPERATING ENVIRONMENT

The next step is to determine how the operating environment will affect an organization's plans and policies as well as the adversary's motivations, capabilities, and activities. This step integrates the organization's operational cyber intelligence and cybersecurity teams. Both teams focus on evaluating their cybersecurity structure, conducting the threat assessment based on relevant factors in the operating environment, and evaluating changes to the operating environment. These can all be considered part of the larger organizational planning effort. Resources should be allocated in such a way that an organization can quickly respond to malicious activity.

There are trade-offs between the business risks and security risks of modernizing security infrastructure, doing nothing, and all points in between. The cost of infrastructure overhauls

can be daunting. Organizations may underestimate the cyber risk, as is common in the retail industry. Yet the very high profile attacks on Target and Neiman Marcus, which compromised more than 70 million consumers, highlight the need to balance business and security risks.⁸

These events have prompted organizations to explore the business and security trade-offs of modernizing their credit card systems and improving cyber intelligence sharing and collaboration through the creation of a Retail Information Sharing and Analysis Center (ISAC).⁹

Based on the impact of the operating environment, an organization will incorporate into its plans and policies those best practices it believes will produce the greatest return on investment. This can

include improved situational monitoring, enhancing audit practices, strengthening firewalls, investing in a threat intelligence capability, and enhancing intrusion detection. However, it also includes analytic or organizational responses such as altering funds allocated to cybersecurity, reprioritizing existing investments, organizational realignments, and hiring to ensure the workforce can support an organization's cybersecurity objectives. In short, an organization can conduct gap analysis to identify their vulnerabilities and again assess the business and security risks of potential responses to the evolving cyber operating environment impacts, which include loss of top-secret security information, stolen credit card data, compromise of the stock exchange or disruption of the electric grid.

EXAMPLE

Protests begin to intensify in Ukraine. Likewise, international rhetoric is heating up between Russia and those supporting Pro-Ukrainian interests (e.g., the US, NATO, EU, etc.). Russia is increasing its military presence on its border with Ukraine.

The Ukrainian president has fled and there is an acting president in power. Russian press is increasing pressure for action and Russian nationalist hacktivist groups are discussing the situation in online forums. Pro-Ukrainian media outlets realize that if the current situation holds or worsens, they are targets for malicious cyber activity. They begin conducting internal reviews of existing plans and policies to determine COAs to reduce their vulnerability to denial of service attacks, web defacements, and false reporting. Media outlets are sharing threat intelligence and some are looking to private security firms for additional expertise.

EVALUATE THE ADVERSARY

Here, the adversary's capabilities, the current situation, patterns of past and current behavior, and specific tasks, techniques and procedures (TTPs) are identified. The organization must evaluate its adversaries on technical and analytic capabilities, and willingness and intent to employ those capabilities. Historical review of past campaigns is essential to uncover adversary TTPs.

A threat matrix (Appendix 1) should be created to prioritize the potential range of threat actors based on their willingness and capability to attack. The threat matrix focuses on threat actors who have already exhibited intent and is used to prioritize resource allocation against the most likely threat actors. It contains qualitative and quantitative evaluation criteria. Examples of qualitative criteria include specific motivations such as: status, financial gain, desire for inclusion in a social or political group, whether the attacker is opportunistic or targeted, and if targeted, the level of persistence.

Opportunistic adversaries search for organization's cyber vulnerabilities. Targeted adversaries are motivated by needs only specific organizations can satisfy.¹⁰ Targeted adversaries can be further characterized by their level of persistence. As organizations continue to improve their cybersecurity, less persistent adversaries will seek easier targets. The most dangerous threats are known as advanced persistent threats (APT)¹¹. Irrespective of an organization's actions, an APT will add resources, seek new vulnerabilities, and develop new capabilities in order to maintain its presence in the organization's networks. Examples of quantitative criteria include the number of attacks attempted, the number of successful attacks, and the location of the attacks, temporal constraints, and financial means.¹²

Evaluation of the adversary can quickly become a data flow and management problem. Various data feeds and monitoring may highlight adversarial targeting strategies. This process will also identify collection gaps and requirements depending on a given adversary. For example, an organization may uncover specific social media sites in which hacker groups congregate. This may require linguistic and cultural support to analyze the online communications. The problem could also fall in the realm of big data with the requirement to filter through a vast data environment to discover anomalies. This quickly runs the seam between tactical and operational level cyber intelligence as an organization needs to track, assess, and formulate a baseline measure of normal network behavior at the operational level. This baseline measure can then inform tactical level anomaly detection. Once an anomaly is identified, the tactical response quickly takes precedence. It would be naïve to assume that an organization would be aware of the full range of known adversaries. Any evaluation of the adversary must accept the possibility of unknown adversarial capabilities.

There are trade-offs between the business risks and security risks of modernizing security infrastructure, doing nothing, and all points in between.

Unlike the first two steps, evaluation of the adversary becomes an I&W exercise of assessing specific external indicators which, if found, are used as a basis for plan and policy review. Information sharing is an essential component of I&W and often requires collaboration between the analytic and technical personnel, both inside and outside the organization. At the aggregate level, evaluation of the adversary also informs more abstract strategic-level decision making. The operational assessment should provide a means to discern trends in adversarial behavior over time. This aids an organization in determining shifts in motivation, intent, and capabilities, which further informs plans and policies.

The Saudi Aramco attacks are indicative of a larger trend of cyber attacks targeting critical infrastructure, but also of the linkage between the timing and target of cyber attacks and the current geopolitical and realpolitik trends within the operating environment. For instance, as tensions rise in the South China Sea, many countries in the region have experienced a rise in cyber attacks on government websites and key infrastructure. In Vietnam, people and organizations associated with energy and natural resources have become the targets of alleged attacks from China.

DETERMINING ADVERSARIAL COURSES OF ACTION

This step aggregates and frames information to identify conditions in which organizations may be more likely to be targeted. At the operational level, this includes areas of likely attack interest, general attack formulas, and adversarial objectives. Identifying the fact that a particular group is conducting a distributed denial of service (DDoS) against an organization or that hackers have a significant interest in specific information regarding business negotiations are key discoveries that allow for tailored response options, increased situational awareness of specific government and corporate resources, and a greater ability to enhance leadership decision making.

The output from COA analysis includes detailed analyses of adversaries and their plans against specific objectives in the short and long term that would allow decision making to deter, detect, and defend. These are generally termed an adversary's "most likely" and "most dangerous" COA (MLCOA/MDCOA). MLCOA and MDCOA long have been used doctrinally in militaries. Intending to give leadership an understanding of the range of possible adversarial actions, the MLCOA/MDCOA products provide the ability to leverage resources against a range of adversarial possibilities. These products are generally presented in paragraph form.

EXAMPLE

It is essential to comprehend the operating environment in addition to understanding the physical network. The 2012 attacks on Saudi Aramco, the Saudi state-owned oil company, are indicative of how the operating environment impacts the timing of offensive cyber behavior. The Shamoon virus was unleashed at a time when 55,000 employees stayed home to prepare for Lailat al Qadr, an Islamic holy night. The virus was one of the most destructive pieces of malware used in attacks in recent past, requiring Saudi Aramco to replace three-quarters of their PCs. Additionally, Aramco lost vast amounts of data. The hackers, "The Cutting Sword of Justice", who claimed responsibility for the attack, indicated that the attack was in response to Saudi policies in the region. However, American officials believe the virus stems from Iran as a response to Stuxnet.¹³

Intelligence resources must be put in place to confirm or deny each COA. This enables further refinement and characterization of the adversary's actual operations. It also assists the analyst in determining the difference between what occurred and what was expected. This product, generally referred to as area of interests (AOI) and points of interest (POI), provides specific indicators that enable leadership to monitor the adversary and

determine which COA the adversary is attempting to execute.

Though the actual planning and implementation for the collection of each individual AOI and POI is tactical in nature, the decomposition of the overall COA and identifying the indicators are operational in nature and must be monitored holistically.

EXAMPLE

Members of an Anonymous-affiliated cell have communicated their intention to 'steal' from financial institutions during the upcoming Christmas holiday. Under the banner of a broader campaign named 'DestructiveSec', so-called operation 'LulzXmas' is likely to target U.S. and U.K.-based commercial banks with the intention of undermining payment processing, disrupting online banking and ecommerce platforms through the holiday season, and exacting reputational damage on targeted organizations. Probable attack types include web site defacement, SQL database breach resulting in the disclosure of credit card information and customer's personal data, and distributed denial of service attacks (DDoS). Anonymous affiliates will likely leverage readily available DDoS tools and have in the recent past preferred the use of ByteDOS v3.2 along with the well-known Low Orbit Ion Cannon (LOIC) tool. Other popular DDoS tools include Pyloris, Slowloris, High Orbit Ion Cannon and hping.

The use of crowd-sourced DDoS tools very rarely results in major disruption to online banking and e-commerce platforms, though reduced bandwidth during the holiday season could have adverse effects on company profits. Reputational damage and tangible financial losses due to data breach and disclosure can vary in severity and impact, with the most dangerous scenario involving the dump of customer data along with credit card data including CVV codes.

Example AOI/POI include:

- Identified forums where Anonymous users post complaints and future targets;
- IT personnel related to a specific corporate website; and
- Monitoring of social network sites and news organizations to identify increased publicity of a specific corporate website that may express opinions or ideas contrary to those of a hacktivist organization.

EXAMPLE

Based on monitoring Russian hacker messaging boards, the Pro-Ukrainian media outlets have assessed that the ABC and XYZ hacker groups are preparing to conduct a denial of service attack against Pro-Ukrainian websites. These same organizations were involved in attacks against Estonia in which they used specific TTPs to successfully execute denial of service attacks against Estonian media. However, these TTPs have been updated since then to include newer capabilities. The Pro-Ukrainian media outlets are preparing their networks to counter these updated denial of service TTPs.

BUSINESS AND MISSION CONSIDERATIONS FOR OPERATIONAL CYBER INTELLIGENCE

Increasingly, those planning for and conducting cyber defense within an organization seek integrated cyber intelligence that combines physical, logical, information and social layers of the operating environment: the geopolitical, cultural, economic and infrastructure aspects of the global system. This integration is imperative for solid, predictive defense options but can be difficult to develop and implement. If not integrated at the operational level, cyber intelligence operations will fail to produce effective recommendations for organizational plans and policies. Generally, there are a few key considerations when determining the size and scope of an organizational cyber intelligence capability: attack surface, available resources, buy-in and integration, and information sharing.

Identifying the attack surface for an organization will largely determine how much data would need to be analyzed to properly develop and maintain situational awareness. As an example, an organization (even a large one) that is centralized physically or logically would need a smaller intelligence framework to protect its resources. In contrast, a company that covers a larger geographic area would need more resources to effectively manage its situational awareness.

Cyber intelligence is expensive. Analysts properly trained in cyber intelligence analysis generally come from niche disciplines and are difficult to find. Software and platforms that support them cater to this niche and are also generally expensive. Intelligence shows its worth by avoiding loss rather than generating revenue. Therefore, funding is always in competition with business units that generate revenue. An organization must evaluate the opportunity cost of investing in a cyber intelligence capability rather than investing in other areas of the organization. Whether cyber intelligence is produced internally, contracted, or a mixture of both, the strength of the program will be determined by the risk-driven allocation of resources to create and maintain an effective cyber intelligence capability. True value comes from integrating the cyber intelligence and business functions. This enables cyber intelligence personnel to understand, while assessing the cyber risks: what information is critical, for how long that information will be critical, and where it is located. Gaining buy-in for this level of integration takes a concerted effort in both forecasting the costs of inaction and ensuring leadership is aware of successes within the organization.

Competition, liability, and reputation are major challenges to information sharing. Yet, intelligence is generally produced from shared information. Establishing well-defined, operational level relationships with peer organizations in order to share critical intelligence information can significantly increase an organization's ability to protect its assets. Throughout government and industry, sharing organizations are continually being formed. Current examples include Critical Infrastructure ISAC, Defense Industrial Base CyberSecurity/Information Assurance (DIB CS/IA) Framework, Defense Security Information Exchange (DSIE), and Infragard.

Appropriately assessing the attack surface, utilizing resources efficiently, gaining buy-in, and sharing information can go a long way to improve an organization's cyber intelligence and better enable it to identify hurdles that may impede growth at the operational level.

WORKFORCE IMPLICATIONS AND SKILL SETS

An effective cyber intelligence workforce requires a breadth of analytical skills and subject matter expertise to support decision makers, stakeholders, and cybersecurity professionals. There are very few professionals who have been trained specifically as cyber intelligence analysts. Many of those currently specializing in cyber intelligence have either come from a technical background and supplemented their skill sets with training in analytic tradecraft, or they have come from an intelligence background and have gained supplemental training in technical aspects of cybersecurity. The necessary balance of technical and “soft” skills is likely to vary across the spectrum of operational levels (i.e., strategic, operational, and tactical). An operational cyber intelligence capability must be able to bridge the strategic and tactical levels. This requires a sufficient understanding of technical aspects of the cyber domain to support tactical action by cybersecurity elements within the organization while also understanding the organization’s strategy in the context of its current and future operating environments.

Skill sets required at the operational level include:

- Basic knowledge of network fundamentals, encryption, security architectures and principles;
- The ability to assess implants, tools, weaponization, and delivery methods of cyber attacks to evaluate trends and patterns;
- Knowledge of and ability to assess political-, economic-, social-, and technological-related trends and events; and, discern their implications for a given industry;
- In-depth knowledge and application of global historical cyber events and national level responses to inform cybersecurity plans and policies quickly, clearly, and effectively in the context of the organization’s mission and strategy;
- Ability to identify, collect, and assess data and information; aggregate and analyze data and use information analytics; and create and disseminate intelligence products that communicate risks and solutions effectively to different consumers;
- Strong written and verbal communication skills; and
- The ability to understand complex problems while formally presenting them simplistically to a broad range of stakeholders.

CONCLUSION

Operational cyber intelligence connects the strategic and tactical levels of cyber intelligence. It serves the organization’s executive managers as they develop strategy-based plans and policies to defend against potential attacks and broader adversarial campaigns. Operational cyber intelligence protects the enterprise by facilitating predictive analysis of specific threats. It accomplishes this task by following four essential steps:

1. Define the operating environment;
2. Describe the impact of the operating environment;
3. Evaluate the adversary; and
4. Determine adversarial COA.

Defining the operating environment bounds the problem space and identifies areas for further analysis. It considers the range of adversarial actors specific to a given organization as well as the range of socioeconomic, political, and military trends that can impact an organization. Describing the impact of the operating environment determines how the operating environment will affect the organization’s plans and policies as well as the adversary’s motivations, capabilities, and activities. Once the impact is assessed, operational cyber intelligence evaluates the adversary’s capabilities, the current situation, patterns of past and current behavior, and specific TTPs. Finally, the information generated from previous steps is used to determine the MLCOA and MDCOA the adversary may follow.

APPENDIX 1 : GENERIC THREAT MATRIX¹⁴

THREAT PROFILE							
THREAT LEVEL	COMMITMENT			RESOURCES			
	Intensity	Stealth	Time	Technical Personnel	Knowledge		Access
					Cyber	Kinetic	
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

APPENDIX 2

Having presented the Task Force’s view on the operational levels of cyber intelligence, it is instructive to consider how these levels are interrelated through the use of a variety of “lenses.” **Table 1** is intended to shed light onto the relationships among the levels of cyber intelligence and prepare for a discussion on tactical cyber intelligence, which will be the focus of the Task Force’s next white paper.

RELATIONSHIPS AMONG LEVELS OF CYBER INTELLIGENCE			
	STRATEGIC	OPERATIONAL	TACTICAL
Scope	General “Art of the possible”	Industry/Sector Partners, Suppliers, Competitors, Customers, other Trust Relationships	Company “Inside the wire”
Focus	Political, Social, Behavioral	Adversarial Campaign Planning	On-the-network
Consumer	C-suite	Executive Management CIO/CISO	Incident Response Teams
Purpose	Maintain Competitive Advantage	Avoid Distribution	Remediate and Return to Normal Operations
Posture	Proactive	Proactive	Reactive
Interrogatives	Who, Why, Where	When, Where, How	How, What
Time Horizon	Far	Near	Immediate
Kill Chain	Motivation/Decision to Act Determine Objectives	Avenues of Approach Acquire Capabilities Develop Access	Implement Actions Assess Status Restrike
Attack Surface	Geographic Physical	Persona Logical	Logical Devices
Adversary	Opportunistic Targeted (President?) Threat Shirting: timing, resources, target, methods		
Types of Intelligence	Estimative intelligence General intelligence Scientific and technical intelligence Identity intelligence	Warning intelligence Counterintelligence	Current intelligence
Nature of	Non-technical, Contextual indicators Arguments traditional technology-centric Defense-in-Depth/Layered Security approaches	Traditional technologies (e.g., IDS)	
Sharing	Public, Private partnerships; ISACs; Private security reports	Automated means (e.g., IOC, STIX, TAXII)	
Decisions	Driven by organizational Strategy	Driven by risk-based resource allocation	Driven by operational restoral or LE evidence collection
Relevant Artifacts	Organizational Strategy Plans of Action & Milestones Business Impact Analysis Enterprise Risk Strategy	Plans of Action & Milestones Business Impact Analysis Business Continuity Disaster Recovery	

Table 1

ENDNOTES

¹“Operational Levels of Cyber Intelligence,” Intelligence and National Security Alliance, Cyber Intelligence Task Force, September 2013, http://issuu.com/insalliance/docs/insa_wp_cyberintelligence_pages_hir/1?e=6126110/4715911

²“Joint Intelligence Preparation of the Operational Environment,” Joint Publication 2-01.3, FAS.org, June 16, 2009, <http://www.fas.org/irp/doddir/dod/jp2-01-3.pdf>.

³“Strategic Cyber Intelligence,” Intelligence and National Security Alliance, Cyber Intelligence Task Force, March 2014, <http://www.insaonline.org/i/d/a/b/StrategicCyberWP.aspx>.

⁴While the traditional Internet certainly consumes the majority of this space, the ‘internet of things’, which includes a range of devices, appliances, gadgets, and even transportation, is likely to increase in relevance over the upcoming years.

⁵David Clark, “Characterizing cyberspace: past, present and future,” Massachusetts Institute of Technology CSAIL, March 12, 2010,

⁶Cheryl Conner, “Are You Prepared? Record Number of Cyber Attacks Target Small Business,” Forbes.com, September 14, 2013, <http://www.forbes.com/sites/cherylsnappconner/2013/09/14/are-you-prepared-71-of-cyber-attacks-hit-small-business/>.

⁷“M-Trends 2013: Attack the Security Gap,” Mandiant, 2013 Threat Report, http://www.greycastlesecurity.com/resources/documents/2013_M_Trends.pdf.

⁸Elise Hu, “Target Hack A Tipping Point In Moving Away From Magnetic Stripes,” NPR.org, All Tech Considered: Tech, Culture and Connection, January 23, 2014,

⁹Kelly Jackson Higgins, “Retail Industry Mulls Forming Its Own ISAC For Intel-Sharing,” Dark Reading, March 11, 2014, <http://www.darkreading.com/attacks-breaches/retail-industry-mulls-forming-its-own-isac-for-intel-sharing/d/did/1141454?>

¹⁰Tony Perez, “Understanding Opportunistic Attacks,” ScuriBlog, June 8, 2012, <http://blog.sucuri.net/2012/06/understanding-opportunistic-attacks.html>.

¹¹Advanced persistent threats (APT) are a cybercrime category directed at business and political targets. APTs are network attacks in which an unauthorized person gains access to a network and stays there undetected for a long period of time. APTs require high degree of stealthiness over a prolonged duration or operation in order to be successful.

¹²An organization has flexibility in this area, and could break down the components into a threat dossier, as described in Reverse Deception: Organized Cyber-Threat Counter-Exploitation by Bodmer et al. A threat dossier, similar to a threat matrix, contains information on an adversary’s objectives, timelines, resources, risk tolerance, skills and methods, actions, attack origination point, numbers involved in the attack, and knowledge source.

¹³“Pricing the Cow’s Tongue: China Targeting South China Seas Nation,” The Threat Connect Blog, May 19, 2014, <http://www.threatconnect.com/news/piersing-the-cows-tongue-china-targeting-south-china-seas-nations>.

¹⁴Sandia National Laboratories. (2007). Categorizing Threat: Building and Using Generic Threat Matrix (SAND2007-5791). Albuquerque, NM: Duggan, D. P., Thomas, S. R., Veitch, C. K., & Woodard, L. Retrieved from http://www.idart.sandia.gov/methodology/materials/Adversary_Modeling/SAND2007-5791.pdf

ABOUT THE INSA CYBER INTELLIGENCE TASK FORCE

The INSA Cyber Intelligence Task Force was created to promote thought and dialogue on the importance of cyber intelligence. In September 2011, the Task Force published its first white paper, *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*.

The Task Force is co-chaired by John Felker, director of cyber and intelligence strategy, Hewlett-Packard Company, and Geoff Hancock, CEO, Advanced Cybersecurity Group. The Task Force is developing a series on the three levels of cyber intelligence: strategic, operational and tactical. The next installment on tactical cyber intelligence will be published in 2015.

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions. As a nonprofit, nonpartisan, public-private organization, INSA’s ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities. INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.



INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

BUILDING A STRONGER INTELLIGENCE COMMUNITY
901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org