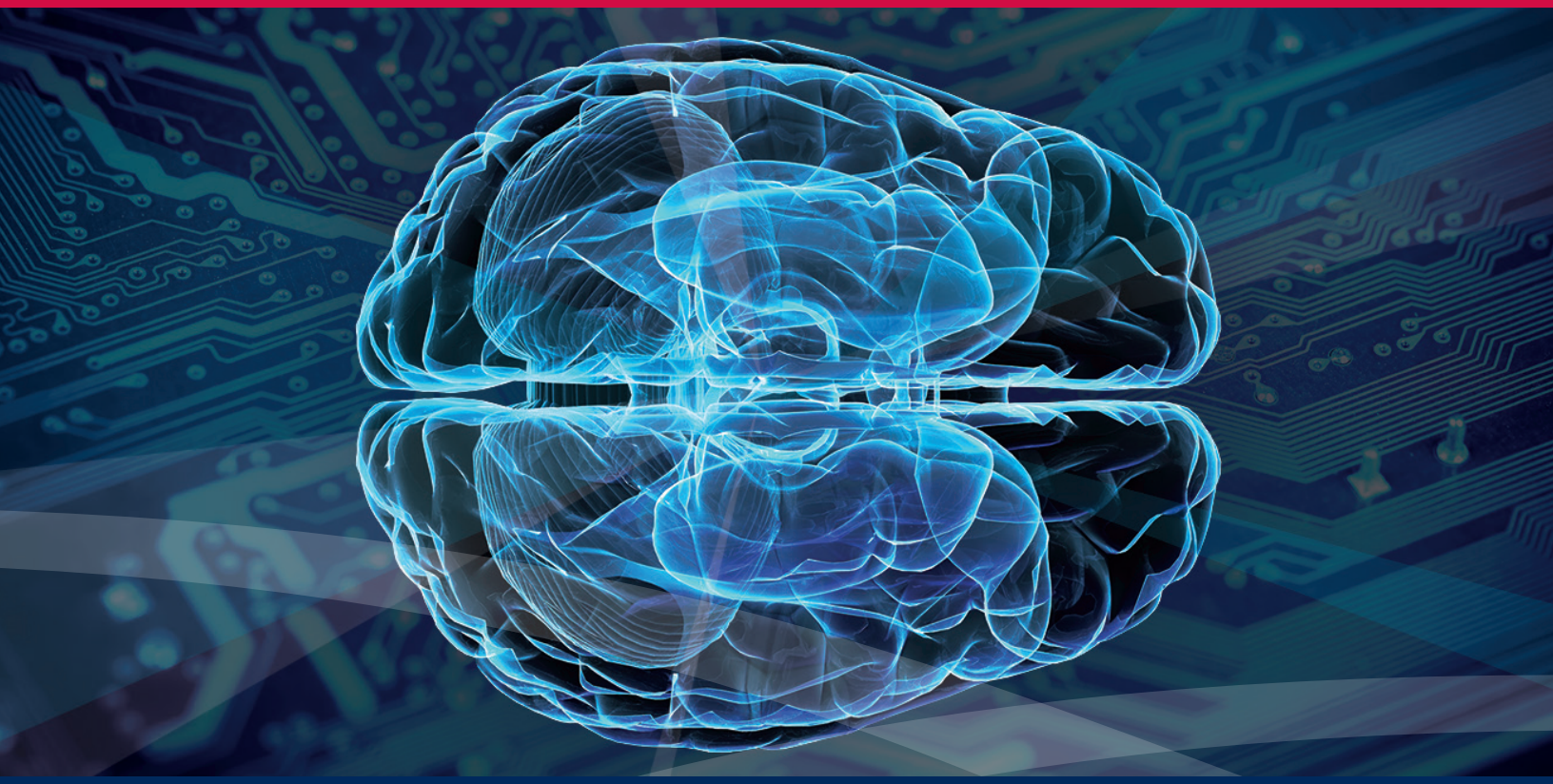

# OPERATIONAL LEVELS OF CYBER INTELLIGENCE

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

CYBER INTELLIGENCE TASK FORCE

SEPTEMBER 2013

INSA

# ACKNOWLEDGEMENTS


## INSA CHAIRMAN
Ambassador John Negroponte

## INSA ADVISORS
The Honorable Charlie Allen, *INSA Senior Intelligence Advisor*

Ambassador Robert Joseph, *INSA Senior National Security Advisor*

## INSA STAFF
Ambassador Joseph DeTrani, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Daniel Allen, *INSA Fellow*

Wanda Archy, *INSA Cyber Research Intern*

## CYBER COUNCIL
Terry Roberts, *TASC, INSA Cyber Council Co-Chair*

Ned Deets, *SEI at Carnegie Mellon University, INSA Cyber Council Co-Chair*

## CYBER INTELLIGENCE TASK FORCE WRITING TEAM
George Bamford, *United States Government*

John Felker, *Director, Cyber and Intelligence Strategy U.S. Public Sector, Enterprise Services, Hewlett-Packard Company*

Troy Mattern, *Technical Director for Cyber Intelligence, SEI Emerging Technology Center, Carnegie Mellon University*

## CYBER INTELLIGENCE TASK FORCE EDITING TEAM
Kristen Dennesen, *Manager, Verisign iDefense*

Tonya Feyes, *Director of Analysis and Research, Endgame Systems*

Richard Howard, *Chief Information Security Officer, TASC, Inc.*

Sean Kern, *Lt Col, USAF, Cyber Security and Information Assurance Department, National Defense University iCollege*

Andrea Limbago, *Chief Social Scientist, Berico Technologies*

Cherreka Montgomery, *National Vice President of Corporate Development, SAP National Security Services*

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

## EDITORIAL REVIEW
Joseph M. Mazzafro, *CSC*

## COPY EDITOR
Elizabeth Finan


Join the discussion for this white paper online using #INSAWhitePaper

## INSA SUPPORTS A HEALTHY PLANET

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

> All operations in cyberspace begin with a human being.

# INTRODUCTION

The September 2011 INSA paper *Cyber Intelligence: Setting the Landscape for an Emerging Discipline* set a framework to approach the development of intelligence in the cyber domain by assessing the cyber threat dynamic, economic costs of cyber attacks and security, and the current U.S. approach to cyber intelligence. The purpose of this paper is to explore cyber intelligence as a disciplined methodology with understandable frames of reference in the form of operational levels. It seeks to inform both government and private industry, with an appreciation for the fact that not all of the relevant decision makers at various levels will share a common view of the challenges associated with conducting business or operations in cyberspace, nor how to best thwart adversarial activity. This paper begins with a brief discussion of what cyber intelligence is and describes the types of events associated with malicious network activity and the proactive operations necessary to prevent or disrupt them. The major themes of this paper are strategic, operational and tactical levels of intelligence that affect cyber operations and cyber security as well as some of the unique aspects of each of those levels. In subsequent white papers, the INSA Cyber Intelligence Task Force will explore in greater detail how entities are actually performing cyber intelligence at each level and how that performance has impacted their operations and security.

All operations in cyberspace begin with a human being. Therefore, while there is not a currently accepted definition for cyber intelligence, it should not be limited to an understanding of network operations and activities. Cyber intelligence includes the collection and analysis of information that produces timely reporting, with context and relevance to a supported decision maker. The information sources used for cyber intelligence are no more limited than they are for any other field that is observed and analyzed by intelligence professionals. Cyber intelligence is not a collection discipline such as Signals Intelligence (SIGINT) or Open Source Intelligence (OSINT); similar to medical intelligence, it is an analytic discipline relying on information collected from traditional intelligence sources intended to inform decision makers on issues pertaining to operations at all levels in the cyber domain. Relevant data to be analyzed may be about network data, ongoing cyber activity throughout the world or potentially relevant geopolitical events. What matters is that it is timely, actionable, and relevant, helping to reduce uncertainty for decision makers. The origin of the data or information is not important. When analyzed and placed in context, information becomes intelligence; and it is intelligence that reduces uncertainty and enables more timely, relevant and cost-effective policy, as well as high-quality operational and investment decisions. This description of cyber intelligence is agnostic with regard to classification or level of information or data set—whether it comes from open source, proprietary, or Intelligence Community sources of information. Ultimately, multiple sources of information are needed by both the private sector and the government to develop a more holistic understanding of the threat environment and enable an effective public-private partnership model. This shared, holistic understanding is a critical element needed to protect shared equities and to enable intelligent actions and useful allocation of resources to ensure an effective defense.

# PROACTIVE CYBER OPERATIONS

In 2012, Norton reported alarming statistics about the growth of malicious cyber activity.[1]

- In 24 advanced nations, 556 million people were victims of cybercrime annually, equivalent to 1.5 million daily or 18 per second.[2]
- Two out of three adults online are victims.
- The cost of cybercrime was $110 billion annually, $21 billion in the U.S. alone.
- Eighty-five percent of these direct financial costs result from fraud, required repairs or patching, theft, and loss of intellectual property.

In the context of this paper the term "proactive" refers to a well thought out and dynamic defense, informed by intelligence, which addresses actual threats.

In October 2011, then-Executive Assistant Director of the FBI Shawn Henry reported one company had determined that 10 years' worth of research and development—valued at $1 billion—was stolen virtually overnight.[3] Clearly, current reactive approaches are not working, and changes in the way we view and operate in cyberspace are necessary. Traditionally, 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. Recent experiences suggest we need to be more proactive.

In the context of this paper the term "proactive" refers to: a well thought out and dynamic defense, informed by intelligence, which addresses actual threats. This includes a consideration of all capabilities within an organization, from network defense posture, to public relations, legal efforts, and other business operations. However, it should not be seen as advocating the use of cyber capabilities by entities outside of government or beyond the perimeter of that network which is legally owned by that entity, even if in defense of their own network(s).[4]

To be more proactive one needs: to understand networks accurately (and in as close to real time as possible); integrate information from networks and other sources; and begin to build a more complete picture of what is occurring and why. This allows for a more proactive position in a dynamic cyber environment. Understanding the elements and value of cyber intelligence at all three levels (strategic, operational, and tactical) and integrating that understanding into the fabric of an organization's operations is not a panacea for preventing cyber threats. It is, however, critical to raising the bar on the provision of secure, effective, and efficient operations. Further, as the lines across

the tactical, operational, and strategic spectrum become blurred, it is imperative that synchronization of the salient elements of each level be undertaken to permit coordinated and informed decision making and operations.

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. Likewise, discussions about intelligence in support of the defensive mission are often limited to network activity itself, as if it were a self-generating activity. It is not. Network activity comprises merely a portion of the total activity-influencing operations in cyberspace. Furthermore, network activity 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." Ultimately, network activity and behavior is driven by human interaction and has a story of intent that can be told, even from open/unclassified sources.

## BEYOND THE NETWORK

The pre-disposition to focus on only a single dimension of cyber defense is a combination of:

- A lack of a full understanding of how malicious cyber actions occur, and
- The tendency, by otherwise highly competent network administrators and defenders, to focus on what they can see on the network.

When these dynamics exist, the result is an almost singular focus on the network to defeat or mitigate what is perceived as only a network challenge and a failure to recognize the series of events that led up to malicious activity on a network. Essentially, the status quo is to be too attached to what is visible on a network, instead of looking outside of a network and complementing that knowledge with additional information. This information needs to be tested by continuously seeking to discover new information and trying to understand the unknown. Cyber threats are not merely a network challenge. As important as the network and understanding what is happening on the network is, there is more that must be considered. Security experts are aware that a series of steps to support decision making must take place within their own organizations before a change takes place. These steps help ensure new changes are appropriate. For example: They must recognize the need to change, they must be motivated and potentially convince others of the necessity for change, they must understand the larger operational impacts of change on the business and missions they support, they must weigh the risks of change, and, if it is required, they may need to coordinate with other operational elements for the down time or training required to implement change. What they cannot do is simply implement changes, even if the security expert believes it is the best course of action. Likewise, there are a series of events that must take place for malicious actor. This area is often overlooked. This is the side that complements the technical data that security experts currently rely on, almost exclusively. This, when combined with current analytic means, is what offers the chance to get ahead.

"Information needs to be tested by continuously seeking to discover new information and trying to understand the unknown. Cyber threats are not merely a network challenge.

# THE KILL CHAIN

Network defenders are beginning to recognize that there is a discernible path, or kill chain, associated with malicious network activity. 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 effect that he intends. Advanced network defense efforts exploit this kill chain to provide temporal distance between the adversary and the defended network. Amin, Hutchins, and Clopperts' *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*[5] is an example of this and a must-read for those interested in network security. Despite the advanced nature of Amin, Hutchins, and Clopperts' analysis and its support to defensive practices, their intelligence-driven scenario requires the malicious actor to be in the defended network long enough to have established a discernible pattern of activity within the network logs. Defenders should utilize these techniques, but they should also not be satisfied with them because the supposition, in order to use these techniques, is that an intrusion has already occurred. A primary purpose of network defense is to prevent intrusions before they occur. To do this, defenders need to expand their understanding of the kill chain beyond network activity.

"Network defenders are beginning to recognize that there is a discernible path, or kill chain, associated with malicious network activity.

A kill chain based on past activity in one's network is very useful. However, what can be truly powerful is when this is combined with knowing what potential actions the adversary could take, based upon intelligence that informs about his capabilities and intentions, and what information that adversary wants before he is inside one's network. 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 in time spans of milliseconds. This implies that references to the "speed of cyber" and the milliseconds necessary for bits of data to traverse the Internet may not be either the only, or the best, temporal model to consider. However, while the movement of malicious files and execution of commands occur at the "speed of cyber," the human-enabled activities necessary to execute malicious cyber operations takes careful planning, choreographed actions, and an investment of time. It more commonly takes days, weeks, months, or even years 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. The time required for that process presents opportunities and thus suggests a different

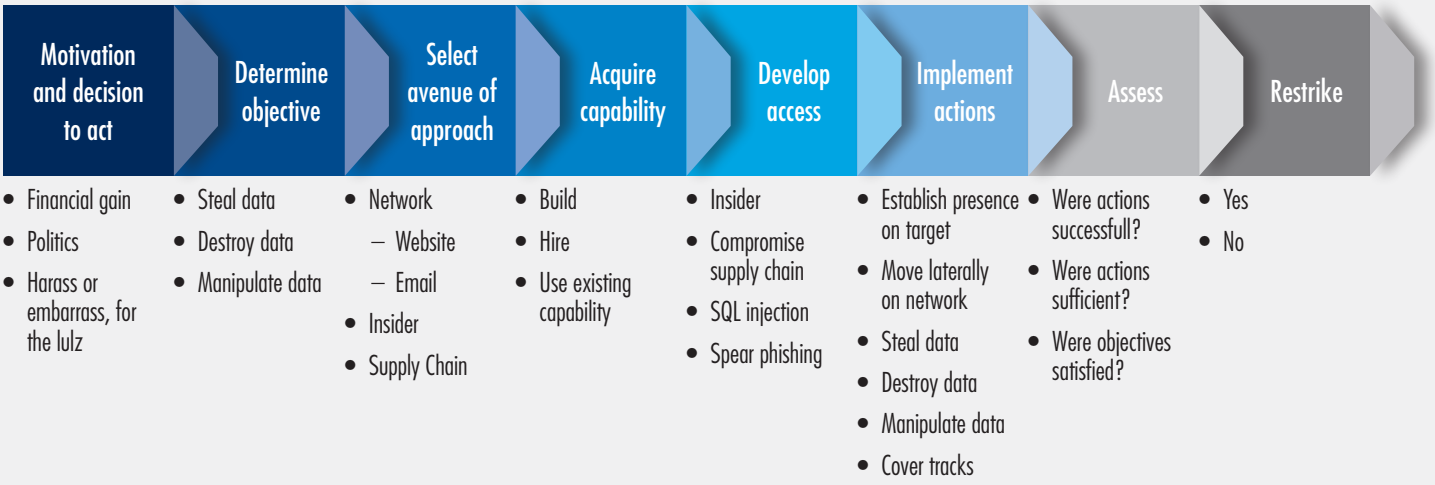


Figure 1: The steps involved from decision to act to execution provide opportunity for defenders to discover and take proactive action. The bulleted examples for each step should be considered as possibilities, not a absolute list of the only options. Cyber intelligence analysts should make assessments as to what are the correct answers for the threats facing them and the missions they are trying to support.

approach. As malicious actors take time to move from decision to execution (Figure 1) that time can also be used by defenders to design and implement an intelligence-based defense.

If one recognizes that the aforementioned steps, or some portion of them, are necessary for a malicious actor, then intelligence efforts can be employed to find out:

- Who may be targeting a network?
- What the malicious actors intentions and capabilities are?
- When will they conduct their activity?
- Where will activity originate?
- How do they plan to penetrate or effect the network?

Malicious actors can range from a nation-state stealing government secrets, to a business competitor trying to gain a market advantage, to ideologically motivated hacktivists. Regardless, each step along the way presents an opportunity to thwart attacks. When these opportunities are sought out and acted upon, it becomes possible to force adversaries to be reactive, imposing additional time and cost upon them. Just as with physical defenses, when the "bad guy" can see that his intended victim is a hard target, and the intended victim changes his defensive posture as the environment changes, the "bad guy" may look elsewhere.

Malicious actors can range from a nation-state stealing government secrets, to a business competitor trying to gain a market advantage, to ideologically motivated hacktivists. Regardless, each step along the way presents an opportunity to thwart attacks.

Even in the case of a motivated actor, options remain. Amins, Hutchins, and Cloppert designed a course of action matrix to consider what ability existed to detect, deny, disrupt, degrade, deceive, or destroy a malicious actor's effort targeting their network (Figure 2). While their examples only considered what actions within the network were possible, the concept is applicable off the network as well. Private companies have other resources available to them, as governments do. For example, a public relations effort can apply pressure or help change how one's company is viewed. Discussions with a key supply chain vendor may help persuade that vendor not to partner with a potential threat to your supply chain.

This begins to challenge the notion that the cost of security is prohibitive and that advantage always lies with the attacker. If the ideas of Amin, Cloppert, and Hutchins are expanded, then a matrix like that of Figure 3, tailored towards the unique capabilities of the user, can be used by friendly actors to help understand what the possibilities are to detect, and then affect, malicious actors before they are in the network.

| 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 | |

Figure 2: Course of Action Matrix from *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf)

| 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 | |

Figure 3: Course of Action Matrix expanding the scope of actions for defenders to enable more proactive measures. Organization CISCO's and CIO's 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.

**Definitions of select terms in Figure 2 and Figure 3 can be found at the end of this paper.*

# THE THREE LEVELS OF CYBER ACTIVITIES

When one considers the decision-making and planning necessary to conduct malicious cyber activity, it becomes easier to understand how it is not simply an "on-the-network" fight. There is no broadly accepted delineation of the various levels of cyber activities. However, it may be useful—and somewhat instructive—to consider thinking of the cyber domain through a framework that is fairly consistent throughout both government and the private sector: Strategic, Operational, and Tactical levels. For simplicity, this paper uses the current Department of Defense definition of these terms from the Dictionary of Military and Associated Terms,[6] Joint Publication 1-02.[7] It should be noted that there is often overlap between the various levels. The intent behind these definitions is to help frame the functions and roles appropriate at the various levels, as opposed to establishing an inflexible structure that is too rigid to meet real world mission requirements or operational realities.

# THE STRATEGIC LEVEL OF CYBER

JP 1-02 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]. Consistent with this thinking, the Strategic level of cyber activity is the determination of objectives and guidance by the highest organizational entity representing a group or organization and their use of the group or organization's resources towards achievement of those objectives. 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 characterization. These are questions that leadership must answer. An assessment of risk and value needs to be conducted; then, a review of the threat landscape should be done. In other words, the organization must determine what the opponent want to achieve and generally how they will attempt to achieve their aims.

Intelligence must be included in the calculus so that strategic-level decision makers can understand the threats that may inhibit or prevent obtaining their strategic objectives.

Such activities, conducted by the adversary 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

Intelligence must be included in the calculus so that strategic-level decision makers can understand the threats that may inhibit or prevent obtaining their strategic objectives. In the government, this certainly includes executives such as the President and his National

Security Staff. It may also extend to the Department of Homeland Security, Federal Bureau of Investigation, unified combatant commands, service chiefs, and cabinet principals. In the corporate world, this is largely the domain of the Chief Executive Officer, the Chief Operations Officer, the Chief Financial Officer, Executive Management Teams, and corporate boards because these individuals establish strategic corporate objectives, policies, priorities, and ultimately allocate the resources. Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) do not typically fall in this realm because while they are critically important to the security and functioning of the networks, most corporate and government environments do not afford these officers the ability to establish broad strategic objectives.

When considering what type of intelligence may be considered of strategic importance, leaders should concentrate on that which reveals new or changed risk with relation to the organization's strategic objectives. Some examples might include:

- The decision by a competitor or potential competitor to enter your market space (e.g., a foreign competitor's new five-year plan now shows interest in developing a domestic capability in a technology your 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 your supply chain.
- Indications that your corporate strategic objectives may be threatened due to adversarial cyber activity.

Some network security professionals may question the value of this information, particularly since it is likely that their analysts would need to perform this function, and it does not provide the type of information typically deemed actionable by network operators or defenders. The reason this information matters is that it will help influence senior executive decision-making on corporate strategic objectives, the appropriate priority of cyber security/intelligence support, and the appropriate allocation of resources towards the security mission vis-à-vis the threats and other operational priorities. There is essentially a return-on-investment decision being taken at the corporate level. Lacking this information, chief executives will most likely prioritize and allocate in favor of other mission functions that appear to more directly and tangibly contribute to attaining strategic objectives. Consequently, cyber security functions are at risk of being funded based upon threat determinations that are made by inadequately informed leadership.

# THE OPERATIONAL LEVEL OF CYBER

JP 1-02 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]. At this level, malicious actors plan their campaigns based upon what they have learned in collecting their own intelligence and on what they had surmised as being necessary based upon their strategic goals. Actors build the capabilities (botnets, malware, delivery methodology [phishing] etc.) needed to support the tactical operations. They maneuver in cyberspace (hop points) to position capability where they need to in order to be effective in their tactical missions. This is the level where a hactivist group may plan both cyber and physical world activities to support their objectives.

“The operational level is where a hactivist group may plan both cyber and physical world activities to support their objectives.

Some examples of operational level intelligence are:

- Trend analysis indicating the technical direction in which an adversaries capabilities are evolving.
- Indications that an adversary has selected an avenue of approach for targeting your organization.
- Indications that an adversary is building capability to exploit a particular avenue of approach.
- The revelation of adversary tactics, techniques, and procedures.
- Understanding of the adversary operational cycle (i.e. decision making, acquisitions, command and control [C2] methods for both the technology and the personnel).
- Technical, social, legal, financial, or other vulnerabilities that the adversary has.
- Information that enables the defender to influence an adversary as they move through the kill chain.

The planning of operations and campaigns to defend against this level of cyber operations is largely the realm of the CIO and the CISO. It is their responsibility to plan appropriate support for new endeavors, temporary or otherwise. It is also their responsibility to ensure allocation of operational information technology systems and security support in order to ensure that corporate/government missions can be accomplished and objectives obtained. Likewise it is their responsibility to understand not just what malware has hit them today, but who is doing it, why, and what their capabilities are so they can stay ahead of the attacks. This is the level that affords opportunity to design defenses, based upon intelligence, against the threats actively, or most likely to be, targeting their network and data—in other words, knowing who and what the threats are BEFORE they are inside the wire. The more informed CISOs and CIOs are about the objectives and capabilities of malicious actors, the better they are able to posture their enterprise to defend against them, thwart their actions, and to be more resilient should defenses fail to effectively mitigate the threat.

# THE TACTICAL LEVEL OF CYBER

JP 1-02 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]. The tactical level of the cyber domain is where the on-the-network actions take place. This is where malicious actors and network defenders maneuver against each other. This is where botnets are directed towards a specific target and then unleash their payload. This is where an adversary finds a vulnerability and infiltrates a network. This is where an actor using advanced persistent threats maneuvers laterally inside the target network, finds the information he wants, copies it, encrypts it, and exfiltrates the data. This is where most of the attention of cyber defense is focused today. While the tactical level deserves attention, the problem with a singular focus on this level means that the adversary is either already in the network, or at the door of your gateway trying to get in. Yet, if appropriate resources were expended in the previous two levels, some of this tactical activity may be precluded (the INSA Cyber Intelligence Task Force will seek to demonstrate this in future white papers in this series).

> The tactical level is where an adversary finds a vulnerability and infiltrates a network.

Typical tactical defensive actions are primarily conducted in the Network Operations Center or Security Operations Center and include: host-based security system alerts, signature or behavior detection efforts, and in advanced cases, some form of kill chain analysis based upon known actors or network behavioral patterns. This level, just as the two preceding it, operates best when informed by intelligence. Consider a Network Operations Center that only knows a window in which they may be targeted for a Distributed Denial of Service (DDOS) attack. This information is obtainable, particularly with some hactivist entities that make little effort to conceal when they intend to strike. Others openly advertise the fact they intend to do so and with analysis of geopolitical events, it is possible to assess the likelihood and timeframe of a nation state doing so, even if acting through proxies. With that intelligence, the "window of time," defenders could coordinate in advance with their Internet Service Provider (ISP) and surge support to reroute traffic coming from high demand request points. Armed with that information, the ISP could potentially help identify and shut down command and control nodes that could limit the severity and impact of the DDOS. This type of pre-coordination and advanced warning alone may make the difference between critical web support services being available or not even if the attack is not thwarted completely.

# CONCLUSION

Cyber intelligence is a complex, as yet undefined, multifaceted approach to framing, thinking about, and reacting to cyber adversarial activity. Many discussions emphasize the complexity of the cyber operational domain, the speed in which activity and operations take place, and the supposed inherent advantage of the attacker. By beginning to define the overall environment and the problem set in manageable operational levels and emphasizing the importance of integrating sound and time-tested intelligence thinking and methodology into the equation, it becomes easier to address the problem. With this methodology, one can better understand and anticipate the adversaries' actions and intent in order to provide the needed and appropriate intelligence at the right time 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 far more than just network functionality. To understand how to support operational level requirements, cyber intelligence analysts will need to understand the human element, what they intend, how they plan, coordinate and execute, and what motivates them towards action or inaction. To support their organization's strategic goals, some analysts will find it necessary 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. Understanding the adversary, whether a nation-state, a business competitor or a criminal organization, understanding one's operational/business environment, understanding one's own exposure (threats and vulnerabilities), and having a clear sense of what is most valuable within one's network, are critical factors in determining resource allocation, analysis of risk and determination of the path an organization will take to achieve its mission. Intelligence is meant to help reduce uncertainty for the decision maker and prevent surprise. Clearly there are more decision makers involved than those in the network operations center. The challenge now is to enable the decision makers, at all levels, to fully understand what information is needed and how to work with their cyber intelligence team to collect it, integrate it and make it accessible to those who must act upon it to thwart malicious network activity. These are some of the questions the INSA Cyber Intelligence Task Force will begin to address in following editions of our Cyber Intelligence Series.

> Understanding, even at a basic level, the cyber "lay of the land" should also help illustrate the need for cyber intelligence analysts to know far more than just network functionality.

# GLOSSARY

**"Chroot" Jail:** A UNIX feature that creates a limited sandbox allowing a process to view only a single subtree of the filesystem. *Binh Nguyen. The Linux Documentation Project. "Linux Dictionary." Accessed 22 August, 2013. http://www.tldp.org/LDP/Linux-Dictionary/html/index.html*

**DEP:** Data Execution Prevention – DEP is a security feature that can help prevent damage to your computer from viruses and other security threats. DEP can help protect your computer by monitoring programs to make sure they use system memory safely. If a program tries running (also known as executing) code from memory in an incorrect way, DEP closes the program. *Windows. "Data Execution Prevention: frequently asked questions." Accessed 22 August, 2013. http://windows.microsoft.com/en-US/windows-vista/Data-Execution-Prevention-frequently-asked-questions*

**Firewall ACL:** Firewall Access Control List – Firewall Access Control Lists (ACLs) make a powerful tool for the firewall administrator to control in a practical way how the firewall treats any IP traffic. *Bitwise Works. "Rule Based Access Control." Accessed 22 August, 2013. http://www.bitwiseworks.com/firewall/access.php*

**HIDS:** Host-based Intrusion Detection System – a method of security management for computers and networks. In HIDS, anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside environment such as the Internet. *Margaret Rouse. SearchSecurity. "HIDS/NIDS (host intrusion detection systems and network intrusion detection systems)." Accessed 22 August 2013. http://searchsecurity.techtarget.com/definition/HIDS-NIDS*

**Honeypot:** A honeypot is a closely monitored network decoy serving several purposes: it can distract adversaries from more valuable machines on a network, provide early warning about new attack and exploitation trends, or allow in-depth examination of adversaries during and after exploitation of a honeypot. *Niels Provos. "A Virtual Honeypot Framework." Accessed 22 August 2013. http://niels.xtdnet.nl/papers/honeyd.pdf*

**In-line AV:** In-line antivirus scanners, typically incorporated into firewalls, look at not just incoming and outgoing SMTP traffic, but also other mail protocols (POP and IMAP), Web traffic (HTTP) and often file transfers using FTP. While in-line antivirus scanners are not as flexible or as reliable as standalone antivirus, they can catch a large percentage of virus traffic and can be a valuable adjunct to both desktop and server-based antivirus deployments. *Joel Snyder. SearchSecurity. "Achieving Network Security with Tomorrow's Antivirus Tools." SearchSecurity. Accessed 22 August, 2013. http://searchsecurity.techtarget.com/feature/Achieving-network-security-with-tomorrows-antivirus-tools*

**NIDS:** Network Intrusion Detection System – a method of security management for computers and networks. In NIDS, anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected. *Margaret Rouse. Search Security. "HIDS/NIDS (host intrusion detection systems and network intrusion detection systems)." Accessed 22 August 2013. http://searchsecurity.techtarget.com/definition/HIDS-NIDS*

**NIPS:** Network-based Intrusion Prevention System. Intrusion Prevention Systems are often deployed to prevent attacks against our assets, including database servers. IPSs do this by monitoring the network traffic for signatures or anomalies and acting on those things they detect. *Jim McMillan. SANS. "Intrusion Detection FAQ: What is the Difference Between and IPS and a Network Based Database Activity Monitor?" Accessed 22 August, 2013. http://www.sans.org/security-resources/idfaq/ips-database-activity.php*

**Tarpit:** allowing a tarpitted port to accept any incoming TCP connection. When data transfer begins to occur, the TCP window size is set to zero, so no data can be transferred within the session. The connection is then held open, and any requests by the remote side to close the session are ignored. This means that the attacker must wait for the connection to timeout in order to disconnect. This kind of behavior is bad news for automated scanning tools (like worms) because they rely on a quick turnaround from their potential victims. *Tony Bautts. Symantec. "Slow Down Internet Worm with Tarpits." Accessed 22 August, 2013. http://www.symantec.com/connect/articles/slow-down-internet-worms-tarpits*

# ENDNOTES

*[1] Norton (5 Sept 2012 ). Norton Cyber Crime Report. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf*

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

*[3] Henry, S. (20 Oct 2011). Speeches [Shawn Henry at the Information Systems Security Association International Conference in Baltimore, Maryland]. Retrieved from http://www.fbi.gov/news/speeches/responding-to-the-cyber-threat*

*[4] INSA takes this position due to the lack of legal structure, both domestically and internationally, which define appropriate levels of force for self-defense in cyber, a lack of legally defensible standards for attribution and a lack of a means to ensure public confidence that when taking such self-defense measures, third party entities would not be inadvertently affected by such action.*

*[5] Amin, Rohan M., Cloppert, Michael J., Hutchins, Eric M., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Proceedings of the 6th International Conference on Information Warfare, Spring 2011. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*

*[6] In order to help eliminate unnecessarily provocative language, and in recognition that not all adversary cyber actions equate to acts of war, the Cyber Intelligence Taskforce elected to omit the word "war" from the levels of war definitions provided in JP 1-02.*

*[7] http://www.dtic.mil/doctrine/dod_dictionary/*


INTEL I
IONAL SECU I
IANCE

## 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 non-profit, non-partisan, 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.

---

## ABOUT THE INSA CYBER COUNCIL:

The INSA Cyber Council is a group of current and former executives from the public, private and academic sectors with expertise in cyber security. The Council engages government and industry communities in pursuit of innovative solutions and thought leadership that will improve existing cyber security policies, practices and organization for both sectors.

## ABOUT THE INSA CYBER INTELLIGENCE TASK FORCE:

The INSA Cyber Intelligence Task Force was created to set the landscape for cyber intelligence by discussing why cyber intelligence is necessary and providing thoughts on how to develop this function in the cyber domain.

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