CYBER INTELLIGENCE

...setting the landscape for an emerging discipline...

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

CYBER INTELLIGENCE: SETTING THE LANDSCAPE FOR AN EMERGING DISCIPLINE

SEPTEMBER 2011

ACKNOWLEDGEMENTS

INSA CHAIRWOMAN

Frances Fragos Townsend

INSA STAFF

Ellen McCarthy, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Jay Fox, *INSA Senior Research Intern*

CYBER INTELLIGENCE TASK FORCE EDITING TEAM

Terry Roberts, *Executive Director, Interagency & Cyber, CMU/SEI*

Bill Studeman, *Independent Consultant*

CYBER INTELLIGENCE TASK FORCE WRITING TEAM

Barbara Fast, *Vice President, CGI*

Michael Johnson, *Senior Scientist/Computer Security Researcher, Sandia National Laboratories*

Dick Schaeffer, *Riverbank Associates, LLC*

EDITORIAL REVIEW

Joseph M. Mazzafro, *Oracle National Security Group*

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

Evolving information systems technology has turned the cyber arena into a multi-dimensional attack space that extends the conventional landscape to a virtual domain where key economic and national security assets are exposed to significant threats. Individual, commercial, national, and international activities interact in this domain, increasing the space for offensive and defensive operations. Cyberspace is a haven for a broad range of disruptive operations, including reconnaissance, theft, sabotage, and espionage. It serves as an environment that allows threats to target hardware, software, financial assets, intellectual property, and individual identities.

This paper is the first in a series developed by the Intelligence and National Security Alliance's (INSA) Cyber Council. It is intended to broaden the vision of senior decision makers in government and industry. Our goal with this paper is to set the landscape for cyber intelligence by discussing why it is necessary and providing thoughts on how to approach the development of this function in the cyber domain. While there is a great deal of focus on current cyber security issues, there is little focus on defining and exploring the cyber threat environment at a higher level. Its unique dynamics and impact on our economy and national security are understudied. In this paper, we will focus primarily on defensive cyber activities. There is a rapidly increasing need to fully leverage cyber intelligence assets and capabilities on a national and global scale to address this ubiquitous, diverse, and evolving group of adversaries. There is also a need to clearly define an emerging cyber intelligence discipline that can be quickly and transparently shared with appropriate private and foreign partners.

The Cyber Threat Dynamic can be broken into three components:

- The Cyberspace Environment
- The Cyber Threat
- The Convergence of the Effects of the Cyberspace Environment and the Threat

The two overarching costs from the cyber threat dynamic are losses due to adversarial activities and the expense of providing and maintaining security. In cyberspace, the low cost of entry and easy access creates an asymmetric environment in which public and private sector organizations incur a disproportionate cost to defend compared to the consequence of attack. While quantifiable assessments of the net impact of cyber attacks are difficult to discern, the cost is great enough to warrant the need for a cyber security apparatus supported by sophisticated cyber intelligence.

This paper assesses the cyber threat dynamic, economic costs of cyber attacks and security, as well as the current US approach to cyber intelligence. Based on these assessments, we believe further discussion on the following topics across industry, academia and government would be a prudent investment in the future security and reliability of the increasingly important cyber domain. These topics include the need to:

1. Systematically define and establish effective cyber intelligence approaches, enduring professions, and needed skill-sets/training/education and technologies
2. Enable the creation of cyber intelligence related policies, approaches, and pilot efforts across industry, academia/non-profits, and government that provide unclassified situational awareness, indications, warning data, analytics, and 24/7 unclassified and classified (as appropriate) reporting to government agencies, trusted industry, and global partners. The Cyber Council believes these pilot efforts are the most relevant value–added recommendations for setting the landscape for cyber intelligence provided by this paper.
3. Establish public-private partnership cyber outreach forums that address these issues/concerns in a comprehensive, practical, and executable fashion
4. Build a meaningful virtual partnership among all relevant agencies and the private sector to ensure seamless sharing of threat information, timely analytical judgments, and reasoned, measured responses to clear threats

Ultimately, effective cyber intelligence will begin to enable predictive, strategic warning regarding cyber threat activities, mitigate risks associated with the threat, enhance our ability to assess the effects of cyber intrusion, and streamline cyber security into a more efficient and cost effective process based on well informed decisions.

INTRODUCTION: TODAY'S CYBER ENVIRONMENT

During the 20th Century, the United States experienced tremendous economic and industrial growth as inventors, entrepreneurs, and policy makers partnered to turn ideas into labor saving and life enhancing technology. During this time period, government and industry needed to collaborate in unprecedented ways in order to serve national interests and meet security requirements.

Advances in information systems technology enabled collaboration among individuals and states regardless of location. Innovation accelerated, and benefits to the United States overshadowed concerns about how these new capabilities might be used for malicious purposes. These same breakthroughs gave unprincipled individuals, organizations, and nations a new range of tools with which to perpetrate theft, fraud, sabotage, and espionage.

A reactive patchwork of technology and processes with the purpose of developing a preplanned comprehensive approach to constructing and using the global network emerged to address the deficiencies created by what was viewed as a temporary fad by these "hackers" and other unsavory interlopers. Historically, government and industry often collaborated on key technological innovations, like nuclear power, to utilize efforts for the common good. Today, government agencies and industry often seem to pursue separate (perhaps counter-productive) policies, in lieu of cooperating effectively to address incoming threats to our local and global network domains.

> The United States as a whole has yet to put in place systemic approaches, tradecraft, technologies, and end-to-end solutions across government, academia, and industry.

The government, as in other areas, has unique insights into the threat space but cannot seamlessly share these insights with the very industries that own and operate over 90 percent of the telecommunications' infrastructure and operations. This is further exacerbated by the common misperception that these threats are technical and tactical level attacks best handled at the unit or individual domain level. This bifurcated approach has resulted in the loss of precious years while the cyber threat vectors and activity levels have grown exponentially. Furthermore, the United States as a whole has yet to put in place systemic approaches, tradecraft, technologies, and end-to-end solutions across government, academia, and industry.

While there is a great deal of focus on current cyber security issues, there is very little focus on truly defining and exploring the cyber threat environment at a higher level, its unique dynamics, and the potential impact on our economy and national security. We need to fully leverage cyber intelligence assets and capabilities to address this ubiquitous, diverse and ever evolving category of adversaries. This white paper addresses the following dimensions of the cyber threat environment:

I. The New Dimension: Cyber Threat Dynamics

II. Impact of Current Levels of Cyber Attacks: The Economics

III. The Role of Intelligence in the Cyber Arena

IV. Areas for Further Discussion and Review

I. THE NEW DIMENSION: CYBER THREAT DYNAMICS

Emerging information systems technology enables the cyber arena to extend the conventional landscape to a virtual domain where key economic and national security assets are subject to threats. The convergence of the cyberspace environment and threat vectors creates a complicated dynamic.

The Cyber Threat Dynamic can be broken into three components:

1. The Cyberspace Environment
2. The Cyber Threat
3. The Convergence of the Effects of the Cyberspace Environment and the Threat

> There is a rapidly increasing need to fully leverage cyber intelligence assets and capabilities on a national and global scale to clearly define the emerging cyber intelligence discipline.

1. THE CYBERSPACE ENVIRONMENT

Cyberspace has become a global commons that has enhanced interaction, information exchange, and productivity. However, it is also a haven for a broad range of disruptive operations, including sabotage, reconnaissance, theft, and espionage. It serves as an environment that allows threats to deny, disrupt, degrade, or destroy hardware, software, and intellectual property.

The Relevance of the "Information Super-Highway."

Although the Internet and highway system analogy may be a bit of a cliché, commerce is instructive when examining the cyberspace environment and the economic impact of cyber intrusions. Imagine if businesses in the United States could not use the interstate system to reliably transport goods. Similarly, in the early days of overseas commerce, ships would often be captured by pirates and bandits who would rob merchants with impunity and little penalty. During World War II, merchant convoys relied on military escorts, which in turn, relied on industry for supplies and innovations. This symbiotic partnership between industry and government was foundational to the economic growth of this nation and the world economy. Today 90 percent of all commerce takes place on the seas, mostly without incident. The Internet has assumed an analogous stature in its role in financial transactions and the exchange of information. Protecting this "super-highway" is a global imperative for the public, private, and academic sectors.

A Multi-Dimensional Attack Space.

The cyber environment, coupled with technology, has created a new multi-dimensional attack space. There is an interconnection between the spatial, physical, logical, and social layers through which the adversary moves with impunity. The complexity of this attack space means that investigators must understand the relationship between these layers and pinpoint the perpetrator's origin and intent in order to gain attribution. With the convergence of computers and telecommunications networks, the defenders must look at this problem as a whole and then disaggregate into its parts. There is a merging of wired, wireless, and optical technologies (networks and RF). Whereas before enterprise networks might be viewed distinctly from hand-held devices or tactical radios, now the cyber network stretches from the enterprise network and its infrastructure to wireless devices being used at the tactical edge by the military, law enforcement, shoppers, or drivers using GPS-enabled devices.

Ultimately, effective cyber intelligence will begin to enable predictive, strategic warning regarding cyber threat activities, mitigate risks associated with the threat, enhance our ability to assess the effects of cyber attacks, and streamline cyber security into a more efficient and cost effective process based on well informed decisions.

Contrary to physical domains and sciences, this environment is truly a complex and dynamic cyber-ecosystem that demonstrates unexpected emergent behaviors every day. Similar to physics in the early 1800s, we are still in the early stages of understanding cyber as a domain and its implications. Cyber science, engineering, and domain are in their infancy, and all are being driven at the speed of continuous technological development. Little is designed with the strategic vision to systematically mitigate threats; much is evolved in a tactical, reactive way. New versions of exploits are launched globally every day, resulting in new vulnerabilities. Given this flaw of software and systems, there is no end in sight to the repetitive iterations of tactical attack and defense.

The Gap Between Law and the Threat.

National and international laws, regulations, and enforcement are still struggling to catch up to cyber activities worldwide. Rules, protocols, and standards are few and disconnected, often conflicting with each other. In most cases, laws have not kept pace with the technical ability of an adversary to move rapidly through national, academic, commercial, and private internet service providers. The lexicon is especially confusing because it remains immature. For example, there is no agreed definition of what constitutes an attack on a nation or a breach of sovereignty. Often theft, espionage, reconnaissance, or even simple hacking is described as an attack.

The Consequences of Outsourcing.

The U.S. government has significantly outsourced significant portions of the design, implementation, and maintenance of Information Technology (IT) to other countries, where our potential adversaries can easily insert themselves into our logistical chains. The United States and other developed countries have outsourced their IT development for economic reasons, but the market is failing to account for the reality of the increased security risk. The present situation is as dangerous as if the United States decided to outsource the design of bridges, electrical

The government has unique insights into the threat space but cannot seamlessly share these insights with the very industries that own and operate over 90% of the telecommunications' infrastructure and operations.

grids, and other physical infrastructure to the Soviet Union during the Cold War. In tandem with the outsourcing of IT development, the IT systems themselves are becoming increasingly complex. Increased system complexity means that there are more exploitable vulnerabilities that arise by accident and more opportunities to hide deliberately introduced vulnerabilities, while it becomes harder for the finite number of trusted experts to check systems for integrity.

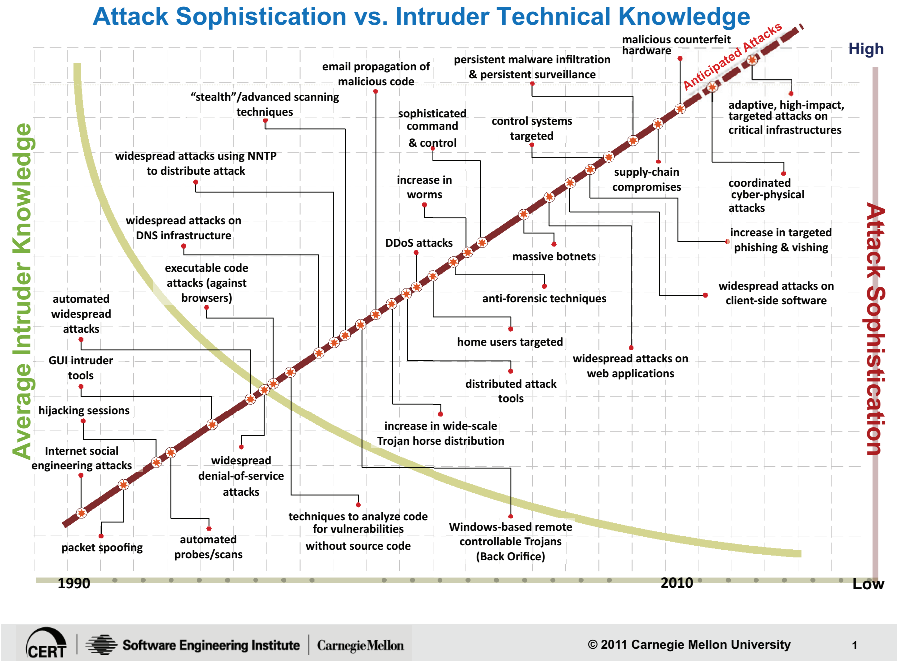

Figure 1: The Evolution of Attack Techniques/Technologies[1]

2. CYBER THREAT

The threats to our national security and economic interests in the cyber arena vary in identity, objectives, assets, and capabilities. Their range can stretch from disruption, to simple theft, to taking down critical infrastructure, to disrupting government functions. The advantage almost always lies with the threat. Ability and intent of these actors become important distinctions to the defender's action.

Varying Profiles.

Attackers do not need to be well educated nor well resourced. They can come from any social cross section. They simply need to have intent and the ability to use technology to perpetrate their activity. Below are a few illustrations:

- Age is irrelevant. Young teenagers in various countries have used the Internet to hack into Pentagon sites.

- Criminals have created international gang activity using the Internet as their medium with drugs, pornography, human trafficking, and financial gain among their activities. Criminals also sell capabilities and services to other criminals, groups, and even states.

- Terrorist groups are using the Internet to conduct their operations, recruit, and coordinate on a larger scale.

- Nation-states are using the Internet to conduct reconnaissance and espionage. Stealing intellectual property is not an uncommon practice among some national governments and state industries. Some states use the Internet to conduct offensive operations as part of their doctrine. These operations include disrupting lines of communication and the target's communications medium. This should be viewed as a new tool in the warfare toolbox—not unlike the advent of armored or aerial warfare.

No Boundaries to Geographic Location or Objectives.

There are no geographic boundaries in cyberspace. Individual, group, and/or nation-state attackers can reside anywhere. Objectives are similarly boundless. Attack motives vary from simple curiosity, personal vendettas, financial or intellectual property gain, and/or a desire to harm an institution or state. Targets include individuals, groups, commercial interests, infrastructure, and nations.

Assets and Capabilities.

Offensive techniques and technologies have rapidly evolved over the past twenty years. Figure 1 illustrates the emergence of new and more sophisticated threat assets and capabilities since 1990. This emergence is based on an improvement in attacker skill sets and more advanced technology at their disposal.

3. THE CONVERGENCE OF THE EFFECTS OF THE CYBERSPACE ENVIRONMENT AND THE THREAT

The heart of the cyber threat dynamic is where the effects of the cyberspace environment and the threat meet. This convergence has a multiplying effect on the vulnerabilities of cyber targets.

> While there is a great deal of focus on current cyber security issues, there is very little focus on truly defining and exploring the cyber threat environment at a higher level, its unique dynamics, and the potential impact on our economy and national security.

Attacker's Familiarity with the Cyber Infrastructure.

Attackers derive an advantage in preparing and executing an attack from their familiarity with the hardware and software the victim uses. The attacker can experiment and perfect an attack on the same commodity infrastructure his victim is likely to have. Part of the cost of using a cookie cutter computing platform has been to give attackers the blueprints to our infrastructure. These blueprints, combined with the complexity of the infrastructure that gives them a place to hide, are all they need. The software architecture is both intricately complex and relatively inexpensive, resulting in economies of scale that complicate cost metrics. We have taken advantage of this economic leverage to such a degree that virtually everyone has a clone of everyone else's infrastructure. A cyber threat retains an advantage due to the inscrutable complexity of IT infrastructure but also to its ubiquity as an inexpensive commodity.

Fostering an Asymmetric Cyber Threat.

The cyber domain encompasses a new and profound dimension of asymmetric warfare. Historically, adversaries of all types have chosen to take advantage of an opponent where and when he or she is weakest, especially if the attacker is outmatched. Because of the attacker's familiarity with the infrastructure, cyberspace offers an opportunity to extend the landscape to a virtual domain where both key economic and national security dynamics are at play. Individual, commercial, national, and international activities all work and socialize in this domain, increasing the space to attack and defend.

In this domain, it is not necessary for a peer-on-peer relationship to be present, nor is it necessary for the attacker to be victorious. The lone individual, the criminal group, or a developing country can be just as dangerous as the well resourced and situated advanced player. The disadvantage lies with states and global commercial interests whose equities rely on the Internet and interconnectivity for national security and economic trade. While every nation is vulnerable, there are places that offer particularly lucrative launch points for the hacker. Failed states enable opportunities for hackers, as they do for criminals and terrorists. These states are simply not resourced, or they are too corrupt to bring governance, law, or order to bear on the issue. There are other nations that tolerate hackers within their borders so long as they are not the victim themselves.

[1] *Terry Roberts. Executive Director Interagency and Cyber, Carnegie Mellon, SEI Cyber Intelligence - Foundational to Cyber Mission Assurance. February 8, 2011*

Exploiting the Current Defense Paradigm.

As in other forms of asymmetric warfare, a perimeter defense is not effective. In cyberspace, it is all the more challenging with the extra obstacles of time, technology, laws, and attribution, among others. Attackers continue to migrate from less sophisticated denial of service operations to very complex attacks. The Stuxnet attack on select networks that operate centrifuges in nuclear facilities provides an example. Attackers now assume legitimate identities to illegally procure intellectual property and conduct other operations. Attackers also insert command and control code that lies in wait inside a victim's network until activated to conduct a pre-designated activity. They are increasingly able to manipulate the content of information in order to meet their objective and influence the actions of the victim. All of these actions can be easily perpetrated from locations thousands of miles away at a time of the perpetrator's choosing with chilling effect.

Because of the attacker's familiarity with the infrastructure, cyberspace offers an opportunity to extend the landscape to a virtual domain where both key economic and national security dynamics are at play.

Time Favors the Attacker.

The dimension of time has changed the threat environment, favoring the attacker. Attacks from around the globe happen in seconds, transiting through multiple waypoints that often mask their movement to the victim. The lack of geographic boundaries permits optimized, virtual routing to the destination. If the attacker is successful in breaching a network's perimeter, the attacker can move quickly, slowly, or lie dormant, depending on the nature of the victim's network and intruder's intent. Additionally, as the speed of networks increases, it allows the perpetrator to maintain the initiative. The hacker can take full advantage of the speed of hardware, software, and communications technology upgrades to expedite his/her attack vectors. The defender is continuously in a game of catch-up. As the defender identifies new attacks and implements new security measures under ever tighter timelines, the attacker simply continues to outrun these measures. For example, some criminals now sell an instant identification service of ongoing on-line transactions to customers who then are able to steal money in that same time space.

Shared Threat and Shared Responsibility.

Today's cyber threat dynamic is a shared threat among public, private, and government entities. This common threat creates additional and unprecedented risks, realities, and vulnerabilities. The attacker can use the same mechanism to strike multiple targets. Civilian "casualties" and collateral damage are very likely. For example, attacks on critical infrastructure, like electricity, can have second and third order effects on hospitals, emergency services, and other unintended victims. Cyber threats can breach touch-points between government unclassified and classified systems. In the absence of a completely new Internet architecture, the public and private sectors are intrinsically linked, interdependent, and must collectively devise and adopt solutions to be effective.

Cyber science, engineering, and domain are in their infancy, and all are being driven at the speed of continuous technological development. Little is designed with the strategic vision to systematically mitigate threats.

II. IMPACT OF CYBER ATTACKS AND COST OF CYBER SECURITY: THE ECONOMICS

The two overarching costs from the cyber threat dynamic are the losses due to an intrusion and the expense of providing and maintaining security. In the cyber environment the low cost of entry and easy access creates an asymmetric environment for "piracy and plunder." Anyone with a computer can be a pirate whether he or she is working for a state government or out of his/her garage. In 2003 estimates of losses due to cyber attacks ranged from $13 billion to $226 billion.[2] While these estimates are often challenged, the impact is certainly significant, and the key risks and costs we incur by not effectively addressing the breadth of threats to the cyber domain must be addressed.

AMBIGUOUS ESTIMATES OF ECONOMIC COSTS.

The first challenge we face is determining the quantifiable effects of cyber attacks and security. The absence of accurate damage assessments is a critical shortcoming. Many researchers have published diverse estimates of the actual and potential economic costs. Kshetri (2010) quotes an FBI/McAfee study as estimating US costs of cybercrime at $400 billion annually.[3] Anderson (2010) estimates the potential losses from a successful cyber attack on the UK's petroleum infrastructure to be on the order of hundreds of billions of dollars.[4]

The impact on business, government, and individuals from cyber attacks has progressed significantly from distraction and moderate disruption to an inability to operate or communicate for days. Typically in commerce, the potential for dishonest interactions and financial losses has been coupled with the recognition that this could be quantified, managed, and included as a business cost. However, cyber disruptions are not always correlated to IP losses, financial theft, or IT sabotage. This clouds the impact and increases risk to businesses and governments. We have advanced beyond mere "acceptable levels of loss" to levels where effective ownership of an individual's, company's, or country's finances, operations and intellectual property may be at stake. The impact has increased in magnitude, and the potential for catastrophic collapse of a company has grown. However, it is not yet clear that the business community understands or accepts this increase in risk. The bottom line is that we are not effectively or comprehensively collecting and assessing key data points to tell us this important story – the cumulative impact and cost of all of our respective government and industry losses of intellectual property and personal data.

> We are not effectively or comprehensively collecting and assessing key data points to tell us the cumulative impact and cost of all of our respective government and industry losses of intellectual property and personal data.

[2] www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf. [3] Kshetri 2010. [4] Anderson 2010.

CRITICAL INFRASTRUCTURE: A SECURITY IMPERATIVE.

Today's cyber threat dynamic is a shared threat among public, private, and government entities.

Critical infrastructure is at significant risk to this form of warfare. Much of the world's critical infrastructure, including in the energy, finance, and transportation sectors, was created and netted before the security imperative became apparent. Even if the infrastructure has modernized security features, it remains vulnerable to attackers who find entry via legacy software that provides trap doors into the larger, modernized network.

RISKS TO IDENTITY AND INFORMATION SECURITY.

Legitimate IT users must constantly question whether the equipment is leaking their information. Average users are becoming more aware that the first time they may know of exfiltration of their data is when they read it in the news or when an adversary uses it against them. Today, users must choose either to keep their information "off the grid" or to take an unquantifiable risk that it will end up in the wrong hands. The cost of losing proprietary or personal information must be constantly considered alongside the opportunity cost of sequestering information from our networked IT infrastructure. Likely, it is the most innovative, sensitive, or insightful (and thus useful) information that has the greatest need for legitimate, but controlled, sharing. Unfortunately, this information is often either over-controlled or too easily accessible. This continuous set of choices is very real and costly in time, technology, management, and bureaucracy.

THE THREAT STAKES ARE HIGH AND EVER INCREASING IN THE CYBER DOMAIN.

At the high end of the threat spectrum, national survival could potentially be at stake in the most extreme circumstances. Our dependencies on net-centricity, IT and telecommunications, and the related microelectronics and paths that facilitate information age processes have become vulnerabilities for virtually all modern states. Using the broadest definition of "cyber" as part of information operations, including both the kinetic (e.g. EMP) and non-kinetic threats to our modern decision and control processes, and by adding our increasing vulnerabilities in space, worst case attack or warfare scenarios at the high end of conflict can mean the complete breakdown of daily life as we know it. Simulations of a weaponized cyber attack against our global telecommunications executed against military and government systems, industry, and critical infrastructure portend the significant risk associated with our dependency on information age systems. At the mid-point of the threat spectrum, there are potential losses of trust in the decision, control, and execution functionality we have come to associate with modern precision engagement warfare. At the lower end of threat, ideas, data, and resources are stolen; functionality is hacked; service is denied; and privacy and civil liberties are violated. Our lives and institutions can generally be disrupted, probed, and exposed.

Impacts and risks our society faces based upon today's incoming cyber threats include:

- **Theft Resulting in Loss of Federal Resources.** This could result in "the release of sensitive or classified government information; the disruption of critical information; and the undermining of agency missions."[5] This fundamentally threatens our national security.

- **Disruption of Our Nation's Telecommunications.** Our nation's prosperity depends on assured and highly performing information systems. The reliance of stock markets and financial institutions on the Internet and associated networks, as well as the operational requirements for command and control by our diplomatic, military, and intelligence organizations identify our digital infrastructure as a critical national security asset. The President has pledged to make this infrastructure "secure, trustworthy, and resilient."[6] Cyber threats expose this infrastructure to significant risk.

[5] Montalbano 2010. [6] Goldsmith 2010.

- Increased Vulnerability to Our Critical Infrastructure. We continue to push initiatives for deeper integration of information systems of all sorts (e.g., energy "smart grid," medical records, and air-traffic control) with the Internet.[7] This integration is driven by powerful economic incentives on the part of both business and government.[8] This integration creates the possibility of a multiplier effect of cyber attacks.

- Short-Term Goals Versus Long-Term Vision of Cyber Security. In the early days of the Information Age, government and industry reaped the benefits of productivity and economic gain associated with IT and the Internet. However, they have probably not sufficiently invested in properly securing these critical infrastructures. We will experience long-term costs if these systems are disrupted or incapacitated. Security vulnerabilities in information technology represent a market externality because the costs from insecurity are either not borne by the party best able to address them (PC industry, cell phones) or do not fully represent the cost to society (critical infrastructure)[9]. Economic incentives of industry are aligned against sharing of information about security threats and actual security incidents.[10] As an example of one kind of disincentive, the share price of companies reporting a significant cyber breach fell an average of 1 - 5 percent.[11]

A REACTIVE AND COST INTENSIVE APPROACH.

Significant time and resources are spent in cumulative attempts to address the latest threat vector and to improve cyber security. Federal Information Security Market, 2010-2015, indicates that demand for vendor-furnished information security products and services by the U.S. federal government will increase from $8.6 billion in 2010 to $13.3 billion in 2015 at a compound annual growth rate (CAGR) of 9.1 percent.

These huge government expenditures result in only momentary benefit because the threat vectors are moving at the speed of technology, and our current, reactive approaches cannot keep up. Examples include distributing "up-to-date" malware signatures when much of today's malware presents a unique signature for every infection; searching for an "optimal" operating system security configuration and then replicating it in a monoculture across a large network; conducting thousands of hours of "extensive" testing that covers only a small fraction of a system's total space; and imposing new programming paradigms in the mistaken belief that they can eradicate vulnerabilities from software.

> The reliance of stock markets and financial institutions on the Internet and associated networks... identify our digital infrastructure as a critical national security asset.

INEFFICIENCIES OF THE CYBER ARMS RACE.

Attempting to secure our systems under current cyber practices is a costly, ineffective, and never-ending struggle. We must avoid an offensive-defensive cyber "arms race" which consumes extensive resources, yet fails to produce an enduring or definitive outcome. At best, adversaries struggle for strategic parity, with one ending up bankrupt and all having little to show for it. At worst, an adversary conceives of the problem from a different perspective (unbeknownst to us), and we are blindsided through technological surprise.

We need to systematically collect key metrics on all of the above activity levels from government and industry so that the real impact is known and the top risks identified can become the priority for resolution. The irony of reporting the impact of a cyber breach is that reporting also puts the company or government agency "on report" to all. Therefore, this key data should be collected by a not-for-profit, trusted third party, and the trends and the cumulative impacts should be shared with all in a non-attributable manner.

[7] Goldsmith 2010. [8] Anderson 2010. [9] Anderson 2010. [10] Anderson 2010. [11] Cashell 2004.

III. THE ROLE OF INTELLIGENCE IN THE CYBER ARENA

The previous two sections have addressed the cyber threat dynamic and the impact of cyber attacks and security. As in any form of security, intelligence is a key component of tactical and strategic decision-making. Effective cyber intelligence will enhance our ability to assess the effects of cyber attacks (a critical shortcoming identified in the previous section), mitigate risks associated with the threat, and streamline cyber security into an efficient and cost-effective process based on well informed decisions.

Effective cyber intelligence will enhance our ability to assess the effects of cyber attacks, mitigate risks associated with the threat, and streamline cyber security into an efficient and cost effective process based on well informed decisions.

DEFINING THE THREAT INTELLIGENCE MISSION (A PHILOSOPHICAL TUTORIAL).

The role of intelligence in any capacity is to collect, analyze, and produce information to provide complete, accurate, timely, and relevant threat assessments to inform decision makers who act on the information. It is usually most effective when it is disseminated at the lowest possible classification level for the maximum number of relevant users facing these threats. In performing this mission, the intelligence agencies seek to penetrate actual or potential threat targets consistent with national strategic, operational, and tactical priorities. These agencies then seek to produce intelligence on adversary or threat capabilities and intentions in a manner that "connects" with the maximum number of relevant customers.

THE ROLE OF THREAT INTELLIGENCE PROCESSES TO DRIVE ACTIONS.

Intelligence and threat analysis does not exist for its own purposes. When threat details are suppressed or ignored, national security incurs significant consequences. It is important to sustain a high level of performance in the dynamic cyber arena. This environment is where threats develop rapidly and are fueled by new concepts for the use of pervasive IT. New waves of innovative capabilities seem to break over users in tsunami fashion, be it the coming cloud architectures or the continuing revolution in personal devices connected to the networks. Given this relentless and constantly unfolding environment, intelligence might be successful in keeping pace with technological innovation. Conversely, it might be slow, or even wrong in its assessments of the threat dynamic. It is therefore important to evaluate public and private cyber intelligence activities that support these security missions in a strategic manner.

THE "CYBER INTELLIGENCE COMMUNITY."

This unique, currently ad hoc, community is made up of government, telecommunication and internet providers, CERTs, and other formal information security entities, specialty companies, and vendors. The members of this community engage in a myriad of activities that could be the potential victim of a cyber threat. This "Cyber Intelligence Community" is currently an informal coalition of the willing that collects and analyzes unclassified and classified cyber intelligence data and trends. There is no formal mechanism across industry and government cyber intelligence entities that successfully collects, processes, and analyzes all identifiable key cyber threat behavior and reports it at an unclassified or reasonable classification level to all appropriate customers. An effective connection between intelligence provider and the customer means that the customer has understood and internalized the intelligence resulting in action to work the intelligence and mitigate the threat. Good intelligence professionals relentlessly

The "Cyber Intelligence Community" is currently an informal coalition of the willing that collects and analyzes unclassified and classified cyber intelligence data and trends.

pursue interactions with customers to ensure that: the data is collected, analyzed, and conveyed; the intelligence serves customers' purposes; and some action is being taken (or deliberately not taken). This cycle can be referred to as a constant process of story-finding, story-telling, story-updating, story-listening, and story-heeding. A concept to institutionalize this ad hoc community is currently missing.

CYBER CONFLICT DOES NOT EXIST IN A VACUUM.

The Joint Chiefs of Staff Pub 1 (unclassified) definition of Information Warfare integrates Electronic Warfare/Attack, Computer Network Operations (for Offense, Defense, and Exploit), Military Information Support Operations (MISO) (previously psychological operations), operational deception, and operational security. These operations can be kinetic and/or non-kinetic. There are adjacent definitions for Strategic Communications, Space-related missions, Covert Action, etc. When these missions are successfully integrated together by a capable adversary in time and space to create the maximum effects, the results can be devastating. The cyber arena has these universal adjacencies and overlapping considerations which intelligence managers must take into account for offensive planning and execution, as well as in building and operating defensive resilience and response.

INVESTING IN CYBER INTELLIGENCE TRADECRAFT, SKILL SETS, AND CAPABILITIES.

A substantial and continuing investment in cyber intelligence should be a strategic imperative in the information age. It is also imperative to use that intelligence to safe guard our ability to maintain security. We must ensure that stable domestic and international economies are not jeopardized by possible conflict with rival powers, rogue states, failing or failed states, modern terrorists and thieves, and WMD proliferators. All formal and informal intelligence disciplines contribute to these imperatives, including Signals Intelligence (SIGINT), Human Intelligence (HUMINT), Open Source Intelligence (OSINT), Geospatial and Measurement Intelligence (GEOINT), and the volumes of unclassified network data and behavior being watched by global CERTs. Continuous liaison among all related parties is critical so that sharing is seamless. This ensures an evolving, improved level of insight and reporting to an increasingly secure and highly performing cyber environment for all.

This evolving cyber intelligence tradecraft requires deep and powerful technical and analytic expertise at all levels. Such technical talent and related capabilities remain ill-defined and in short supply across government and industry. An institution that has made some headway in this regard is the Information Assurance Directorate (IAD) at the National Security Agency. IAD is the front line of the defensive cyber mission. It commands substantial resources, high performing talent, strong processes, and informed outreach. It also works hand in hand with military, public, and private partners to ensure that our cyber capabilities and intellectual property are defended and that our defense is informing offense and vice versa. IAD is a good start, but we must emulate their good practices and innovativeness in defining professional attributes, associated education, and training goals for the unique career fields associated with the cyber realm.

The vast majority of the dangerous activity occurs within the .com domain (as opposed to the .gov or .mil domains) and over 90 percent of the threat data and analytics are unclassified. Therefore, as a nation, we have systematically relegated the identification, tracking, and reporting of this threat to the network operations arena and IT professionals without the inclusion of the invaluable expertise and the analytic tradecraft of the U.S. Intelligence Community.

IV. AREAS FOR FURTHER DISCUSSION AND REVIEW

Our national ability in the area of cyber intelligence remains unclear. There is evidence that we are collecting effectively in this complex area. There is sound open source evidence that we are acquiring significant cyber and information warfare capabilities. Unfortunately, as a nation, we remain exposed and vulnerable to focused cyber threats. The uncertainty associated with this situation raises many questions including:

Does the rush to play in the capability and profit arenas of Information Age markets simultaneously drive us to a potential abyss, by causing us to ignore, play down, over-classify, or restrict the inconvenient cyber truths required to have information security and assurance concurrently?

Are our innovative endeavors so focused on markets and functionality that we cannot simultaneously innovate to some low, medium, and high levels of information security and overall hardening in the process?

Has intelligence done a sufficient job of informing the community and public on cyber threats writ large?

One can infer the answer to these questions is negative since there is a universal clamor in many concerned public and private quarters that more needs to be done to distribute timely threat data, situational awareness and warning. This needs to be data that has specific details, not just data at a high level. The U.S. military has been so overwhelmingly superior globally against niche adversaries who threaten in certain dimensions that we have not had to face the comprehensive specter of real cyber warfare. Literature has been full of stories of looming or developed threats which, under the worst circumstances, can have grave implications for defense and national critical infrastructure in terms of conflict and crisis functionality.

Virtually the entire U.S. Intelligence Community (working with extended partners) is involved to one degree or another in cyber threat matters. The means exist, albeit often at the classified levels, to collect, analyze and produce estimative and fact based data on both an in-depth research analysis basis or as current intelligence. Some organizations like NSA, CIA, DIA, DHS and the military services are more involved than others. However, the actual handling and security classifications of threat information are pervasive problems in disseminating cyber intelligence. New ways need to be found to clear those who need to know, quickly sanitize the

As a nation, we have systematically relegated the identification, tracking, and reporting of this threat to the network operations arena and IT professionals without the inclusion of the invaluable expertise and the analytic tradecraft of the U.S. Intelligence Community.

data, or not classify information to maximize the widespread and detailed effectiveness. Classification should only be used when there is a requirement to protect sources and methods or as it relates to our own attack or exploit means. We need to develop sharing concepts on both threats and solutions, so that every effort is expended to disseminate the details to federal, state, local, tribal, private, and key foreign partners.

We must consider a national intelligence consortium or federation and defined public-private partnership concepts, which could implement an effective continuous capability of collecting, organizing, analyzing, disseminating and leveraging threat intelligence.

DEALING WITH LARGE-SCALE, COMPLEX NATION-STATE OR MARKETPLACE PROBLEMS.

Organizing for success is the key, and it should be underpinned with strong governance to drive and/or track results. Overall, we must consider a national intelligence consortium or federation and defined public-private partnership concepts, which could implement an effective continuous capability of collecting, organizing, analyzing, disseminating and leveraging threat intelligence. This cannot be left to the formal U.S. defense and intelligence communities alone because their equities exist on narrower national security lines. Additionally, the U.S. government has only a limited role in developing the current family of digital age software, hardware, and global telecommunication networks being used or designed for the future.

IDENTIFYING THE CUSTOMERS.

Assuming we will optimize the creation and dissemination of cyber intelligence at every appropriate level, we need to understand the customer set for threat intelligence. This is a key question because if there are to be strong connections between government and industry partners, we must define, understand, and establish their respective roles and alignments to create a cyber intelligence consortium analyzing and reporting current threats and serving customers.

We need to develop sharing concepts on both threats and solutions, so that every effort is expended to disseminate the details to federal, state, local, tribal, private, and key foreign partners.

CONCLUSIONS.

In response to the preceding paragraphs, we make the following suggestions across industry, academia and government.

Overall, we must consider a national intelligence consortium or federation and defined public-private partnership concepts, which could implement an effective continuous capability of collecting, organizing, analyzing, disseminating and leveraging threat intelligence.

1. Continue to promote discussion, debate, and action on systematically defining and establishing effective cyber intelligence approaches, enduring professions, needed skill-sets/training/education and technologies:
   - Development of strategies (beyond current "patch and pray" processes), policies, doctrines, legal frameworks, and overall global context for cyber intelligence matters
   - Increase global business, diplomatic and other forms of engagement, which should discuss potential ways to create more stability and mutual security in the cyber arena in order to reduce the potential for cyber conflict, theft, sabotage, and espionage
   - Support development of deterrence, dissuasion, and other high level concepts and measures for maintaining peace and stability at all levels of conflict and crisis
   - Define cyber intelligence professions, needed skillsets, training, and education for both industry and government needs
2. Enable the creation of cyber intelligence related polices, approaches, and pilot efforts across industry, academia/non-profits, and government that provide unclassified situational awareness and indications and warning data, analytics and 24/7 unclassified and classified (as appropriate) reporting to government agencies, trusted industry, and global partners:
   - Corporately define specific activities, plans, and intentions of adversaries; continuously identify current and emerging threat vectors, and support our plans and intentions
   - Identify the specific technical means utilized or planned for cyber attack operations in deep technical detail to include supply chain issues, paths to be exploited, nature and character of deployed infections, systems/product weakness, effects, and anticipated planned or ongoing adjacent activities
   - Maintain detailed cyber situational awareness writ large
   - Participate in the rapid control and release of cyber means in order to ensure a viable intelligence gain and loss awareness
   - Identify what criminal activities are ongoing or have already happened in cyber networks, do formal damage assessments in these areas, and support development of improved defenses
   - Partner on research and development in the challenging areas of attack attribution, warning, damage assessment, and space related threat collection and analysis
   - Organize and support counter-intelligence and counter-espionage (CI/CE) activities, with special focus on identifying/using auditing tools and processes to deal with the insider threats
   - Create a consistent and meaningful approach for the cyber equivalent of Battle Damage Assessment (BDA)/Combat Effectiveness Assessment

3. Establish public-private partnership cyber outreach forums that address these areas in a comprehensive, practical, and executable fashion. These forums can take the form of commissions that study the demand for cyber intelligence and value added to cyber security.

We believe there is an urgent need to better define and develop cyber intelligence as a new discipline in the IC. Such a discipline will also demand discussion of the unique training, education, skill sets, and tradecraft that will be required to successfully conduct meaningful collection and analysis in the cyber domain.

4. The dilemma that exists in the current cyber intelligence apparatus is that DHS has the authority but lacks the experience and capabilities to orchestrate a comprehensive approach to cyber intelligence. DoD has much of the actual cyber intelligence capabilities, and private industry owns most of the infrastructure. Ultimately, INSA's Cyber Council would like to see a meaningful partnership among all relevant government agencies and the private sector to ensure seamless sharing of threat information, timely analytical judgments, and reasoned, measured responses to clear threats.

As stated earlier, there is clearly a great deal of focus on cyber security issues. Hardly a day goes by without some news of a major hacker attack on government and industry information infrastructure or reports of a significant security breach. The economic and national security ramifications are apparent. Our ability to truly define, explore and analyze this cyber threat environment in a thoughtful, methodical manner at a reasonable level of classification is not yet well developed.

We believe there is an urgent need to better define and develop cyber intelligence as a new discipline in the IC. Such a discipline will also demand discussion of the unique training, education, skill sets, and tradecraft that will be required to successfully conduct meaningful collection and analysis in the cyber domain. These and related topics, such as the role of cyber intelligence in other aspects of cyber operations and who is best suited to develop this discipline, will be the subject of further discussion and white papers by the INSA Cyber Council.

INSA

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

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.

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
SUPPORTING ADVANCES IN THE NATIONAL SECURITY AGENDA

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