ACKNOWLEDGEMENTS

CHAIRMAN
Ambassador John Negroponte

STAFF
Ambassador Joseph R. DeTrani, President
Chuck Alsup, Vice President of Policy
Dave White, Senior Policy Advisor and Resident Fellow
Ryan Pretzer, Policy and Public Relations Manager
English Edwards, Marketing and Communications Manager
William Cullin, Fellow
Hannah Ritz, Cyber Intelligence Intern

CYBER COUNCIL CO-CHAIRS
Terry Roberts,
Founder & President, WhiteHawk, Inc.
Ned Deets, Director,
Software Solutions Division, Software Engineering Institute

CYBER INTELLIGENCE TASK FORCE

Writing Team
Geoff Hancock,
CEO, Advanced Cybersecurity Group
Task Force Co-Chair
Christian Anthony,
Senior Cyber Intelligence and Security Professional,
Johns Hopkins University Applied Physics Laboratory
Lincoln Kaffenberger
Information Technology Officer, Financial Sector

Editing Team
John Felker,
Director of Operations, National Cybersecurity and Communications Integration Center, DHS
Task Force Co-Chair
Blake Moore,
Director of Operations, Security Markets, Splunk
CDR David Di Tallo,
USN, Member and Military Faculty, National Defense University
Andrea Limbago,
Principal Social Scientist, Endgame

EDITORIAL REVIEW
Joe Mazzafro

COPY EDITOR
Christina Ma, INSA Intern
Allison Smith, INSA Intern

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.
Cyber intelligence enables organizations to become better informed about the types of attacks they face, proactively defend against those attacks, and manage enterprise, data and transactional risk more effectively.

INTRODUCTION

Cyber intelligence is the comprehensive assessment of an adversary’s capabilities, intentions, and activities in the cyber domain, and using that assessment to inform an organization’s cybersecurity posture. In this paper, “adversary” could apply to an incredibly broad range of cyber actors, to include both state and non-state entities, as well as transnational criminal organizations, marketplace competitors, and “lone wolf” cybercriminals and hacktivists. The collective thread among them is a motivation to infiltrate an organization’s networks and steal, modify or corrupt data for purposes that could compromise the organization’s security, diminish its commercial footing and/or disrupt its day-to-day operations. Today, cyber is increasingly the domain of first resort for adversaries, who enjoy low costs of entry with high rates of effectiveness. To combat this threat landscape, cyber intelligence enables organizations to become better informed about the types of attacks they face, proactively defend against those attacks, and manage enterprise, data and transactional risk more effectively.

Since 2013, the Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force has presented foundational thinking and approaches to the discipline, paying particular attention to how cyber intelligence functions at the strategic and operational levels within an organization, with white papers published in March and October of 2014, respectively. This paper, the fourth in the series, will concentrate on tactical cyber intelligence, which addresses the daily management of cyber threat data, insights and analytics. In the foundational paper, Operational Levels of Cyber Intelligence (September 2013), we defined the tactical level as “where on-the-network actions take place.” Now, we will examine some of the key elements of a tactical cyber intelligence program.

The goal is to inform government, academia and private industry of areas we believe should be prioritized and specific functions that should be considered when implementing tactical cyber intelligence thinking, analysis and team processes. This paper, and the Levels of Cyber Intelligence series as a whole, can be leveraged as an initial point of departure for organizations as they work to define, refine and implement cyber threat intelligence best practices and approaches.
TACTICAL CYBER INTELLIGENCE & INFORMATION SECURITY MATURITY

Cyber intelligence at the tactical level examines what is happening on the network, focusing on the strengths and vulnerabilities of an organization’s network defenses, and the tactics, techniques and procedures (TTPs) employed by adversaries. The organization’s capacity to accomplish this — and use that intelligence to inform strategic decision making by executive leadership — depends on the maturation of its information security program. Information security maturity is driven largely by the organization’s understanding of risk and the resources committed to mitigating that risk. Information security maturity varies widely from company to company and sector to sector.

Information security maturity models are plentiful, provided by both public and private sector entities, and help guide an organization’s information or network security development. Rather than prescribing to (and extrapolating upon) a single model, here we will identify how information security maturity, generally speaking, relates to an organization’s ability to conduct and benefit from cyber intelligence.

- **Immature information security:** Such organizations place little prioritization on security or have no security-focused tools, expertise or processes. The information technology (IT) team doubles as the security team and is more focused on network functionality than cybersecurity. As a result, these organizations are unable to realize the value of cyber intelligence.

- **Mature information security but without intelligence capability:** These organizations have made network security a priority. They devote considerable resources to securing their network and capturing, recording, and analyzing indicators of compromise (IOCs), which include virus signatures and Internet Protocol (IP) addresses. Some organizations will have an analyst, or at larger organizations, a security operations center (SOC), devoted to monitoring network security systems. Honeynets, a network set up with intentional vulnerabilities, may be deployed in hopes of ensnaring an adversary and gaining a better understanding of its motivation and activities. Mature organizations have threat intelligence feeds monitored by their security team.

- **Robust information security that includes a dedicated cyber intelligence capability:** These organizations likely monitor multiple threat data feeds and conduct formal and informal threat intelligence sharing with other companies in their business sector. Their SOC includes or is accompanied by an established cyber intelligence unit, with analytic and reporting capabilities within the organization. The organization is willing to invest in the additional resources as necessary to keep up with the speed of evolving adversarial technologies and approaches.

Mature information security processes result in actionable intelligence for an organization’s key decision makers. “Actionable intelligence” refers to information that has been integrated, processed and analyzed from various sources so that customers can use it immediately to
meet their cybersecurity objectives. When executive leadership is the customer, cyber intelligence assessments can empower executives to take decisive actions that improve an organization’s likelihood of mitigating or preventing a cyber incident. They also provide critical feedback to the organization’s cyber intelligence managers and operators by helping them understand what information the customer (e.g., executive leadership) is expecting (see figure below).

**CYBER INTELLIGENCE: RESPONSIBILITIES AND INTERRELATIONSHIPS**

---

**STRATEGIC CYBER INTELLIGENCE**

Requires senior leadership to determine objectives and guidance, based on what is known of potential adversaries and what security posture is already in place, in order to successfully assess threats.

**OPERATIONAL CYBER INTELLIGENCE**

Bridges the strategic and tactical levels of operations. Assesses the organization’s operating environment to identify indications and warnings of potential cyber risks.

**TACTICAL CYBER INTELLIGENCE**

Involves specific actions being taken to defend networks against malicious actors attempting infiltration. Relies upon sufficient resources being devoted to the strategic and operational levels.

---

**BENEFITS OF TACTICAL CYBER INTELLIGENCE**

**TACTICAL CYBER INTELLIGENCE BENEFITS ORGANIZATIONS IN THE FOLLOWING WAYS:**

1. **Provides context and relevance to a tremendous amount of data.** Many large organizations have access to terabytes of data without the ability to understand it, filter it and make it useful. At the tactical, day-to-day level, filtering out the noise is crucial. Tactical cyber intelligence introduces methodical processes that help manage incoming disparate data sets, turning them into insightful and actionable intelligence that meets the organization’s threat information needs.

2. **Empowers organizations to develop a proactive cybersecurity posture and bolster its overall risk management policies.** Cyber intelligence at the tactical level must be specific enough to support an organization’s ability to minimize risk. By identifying network and organizational vulnerabilities as well as patterns of adversarial behavior, tactical cyber intelligence can provide insights into an attack model, revealing the areas of highest risk. It also can identify technical, business or mission weaknesses and help define and mitigate an organization’s enterprise risk.

3. **Informs better decision making during and following the detection of a cyber intrusion.** Threat information gathered by system and security logs, amongst other sources, could provide a more complete picture of how an adversary gained or is attempting to gain access to the organization. Indicators of compromise (IOCs) include virus signatures and malware files, IP addresses, and other technical clues of abnormal network activity that can help reveal an adversary’s TTPs, as well as what data had been accessed. IOCs could help reveal an adversary’s identity, intentions and motivations.

4. **Drives momentum toward a cybersecurity posture that is predictive, not just reactive.** A more mature, inclusive and agile cybersecurity framework will allow the organization to collect and analyze more data sets, while complementing the tactical cyber intelligence process. The more inclusive the analyzed data becomes, the more complete the insights are, thereby better preparing an organization’s cyber defense capability against all adversaries.
ESTABLISHING A TACTICAL CYBER INTELLIGENCE PROGRAM

The frequency and severity of cyberattacks on public and private sector organizations demonstrate the need for more resilient, agile, and preventive cybersecurity measures. A posture of standing perimeter defense, no matter how robust, is not a singular solution for today’s adversaries and threat vectors. Organizations that present themselves as difficult targets force the adversary to either go elsewhere or expend greater resources. The goal is to raise the costs for adversaries to implement a successful attack.

As organizations move to a more advanced model of information security, tactical cyber intelligence can be an effective tool when used properly and supported by decision makers at every level. It enables decision makers to streamline information security processes and create procedures that harness the most timely and impactful information available, as well as better allocate analysts and other resources. As momentum builds, companies are able to share IOCs with trusted counterparts, thus strengthening cyber defenses and crime prevention across industries. We recommend four areas that an organization should consider as they create a tactical cyber intelligence program:

- Cyber Intelligence Preparation of the Environment (CIPE)
- A cyber intelligence lifecycle
- Information sharing
- Cyber threat data feeds

CYBER INTELLIGENCE PREPARATION OF THE ENVIRONMENT

Cyber Intelligence Preparation of the Environment (CIPE), alternatively recognized as Intelligence Preparation of the Cyber Environment (IPCE), is derived from the U. S. military term, Intelligence Preparation of the Battlespace (IPB). IPB is an analytic methodology employed to reduce uncertainties about the threat and operating environment, which includes cyber along with air, land, sea, and space. Private sector information networks can be as dynamic today as any battlefield; therefore CIPE easily can be adapted to help corporations and agencies maximize their security posture. CIPE entails four steps, repeated continuously:

1. Define the Technical Operating Environment
2. Describe the Impact of the Technical Operating Environment
3. Evaluate the Adversary
4. Determine Adversary Courses of Action (COAs)
As part of a tactical cyber intelligence program, CIPE is foundational to protecting an organization’s most vital assets. The objective is to provide a holistic understanding of the organization’s operating environment, and threat landscape, as well as reduce any uncertainties across the enterprise. The fewer uncertainties an organization faces, the greater the challenge for its adversaries. Briefly, we will examine these four steps.

1. Define the Technical Operating Environment

This consists of having a complete understanding of your technical network – including information technology, hardware, software, wireless assets and online business processes – and its vulnerabilities and strengths. What is the most valuable data on the network? Where is it and who has access to it? Conducting this type of assessment will give the organization a view of its gaps, risks, shortfalls and priorities. This comprehensive view of assets provides the information necessary to help plan the use of new technology, business or mission objectives.

2. Describe the Impact of the Technical Operating Environment

Understanding how the technical environment impacts the organization’s operations is critical. Knowing how the use of IT and wireless technology influences enterprise risk, business risk, and technical risk can provide the information to develop a cyber baseline, which will inform the organization about where it should apply its resources to be most effective. This baseline should include external environments that are friendly (e.g., partners, customers, supply chain) and unfriendly (e.g., those that present an increased risk or a direct threat to your environment).

3. Evaluate the Adversary

This step identifies and evaluates the adversary’s TTPs, including technical capabilities and limitations, patterns of operation, and potential motives and intentions. Based upon intrusion trend data, models are developed that portray how the adversary normally conducts network attacks and how they have adjusted their methods. Advanced steps may include reviewing adversaries’ TTPs to develop key indicators associated with various threat vectors and criminal courses of action (COAs).

4. Determine Adversary Courses of Action

The fourth step builds upon an understanding of the adversary’s probable intent and future strategy. Some of the information that needs to be gathered includes the adversary’s likely objectives and desired end state, which will require identifying, evaluating and prioritizing each COA at its disposal. The answers often can be found in annual data breach reports, US-CERT reports, and through organizations like the FBI’s local InfraGard or the Internet Storm Center.

BY IMPLEMENTING CIPE, ORGANIZATIONS:

- Identify knowledge gaps, which will drive the information and intelligence collection to fill those gaps. In other words, knowledge gaps become prioritized intelligence requirements.
- Enable an understanding of the complexities that exist within the network and how to improve protection.
- Align traditional computer network defenses with nontechnical operating dependencies, including business partners and customers.
- Reveal an adversary’s capabilities, trends and likely intentions.
- Help the team understand the network and its surrounding environment in order to determine the courses of action an adversary could pursue.
- Provide an understanding of what the adversary can do to inform the development of a prevention, mitigation and response plan.
- Strengthen the organization’s security posture by reducing uncertainties and risk to cyberattacks.
A CYBER INTELLIGENCE LIFECYCLE

The CIPE process establishes the foundation of a tactical cyber intelligence program. Next is the implementation of an intelligence lifecycle, encompassing the processes that will lead to the production of actionable intelligence from the collection and analysis of raw technical and nontechnical data. Intelligence lifecycles vary across U.S. Intelligence Community (IC) agencies, in part because those lifecycles were designed to process many different types of intelligence, including human intelligence (HUMINT), signals intelligence (SIGINT) and geospatial intelligence (GEOINT). They were developed long before advent of the cyber domain and the need to gather “CYBERINT,” information from online platforms and about the actors on those platforms. Those models are now experiencing their own evolutions to better address the 21st century environment. Using elements of both the FBI’s and CIA’s currently adopted intelligence lifecycles, respectively, one can develop a cyber intelligence lifecycle to drive a tactical cyber intelligence program. The seven stages are as described below:

1. Requirements: The first step is identifying the specific information required and what is necessary to acquire it. If the organization is expanding its supply chain or opening new partnerships, the cyber intelligence team could conduct an assessment to determine the status of a new partner’s security posture, whether it has been breached or attacked, and what TTPs were used. Other requests may be more technical in nature, such as obtaining the details and samples of recent attacks, both inside the industry and elsewhere. This would include comparing it to the organization’s own current security posture, then identifying and remediating gaps.

2. Collection: Collecting useful data involves a variety of sources, such as news feeds, paid services, forums, white papers, and even human sources. Participation in cyber threat information sharing venues also greatly enhances collection capabilities. Understanding which sources are likely to be reliable and produce relevant information is a laborious but crucial process.

3. Process and Exploitation: Turning data into actionable intelligence requires an analytic process that is repeatable, easy to implement, and produces valuable insights. A consistent methodology helps structure the data – extracting the relevant information from a larger data set and determining which elements apply to the organization’s assets – and interprets that data into digestible content. By gathering specific IOCs, including IP addresses, domains, URLs, email addresses, file names, and cryptographic hash functions (e.g., MD5, SHA) an analyst can begin turning this data into intelligence. Another aspect is looking for opportunities to create intelligence through synthesis of current data. The goal is to identify trends that can be drawn together into a broader intelligence product for midlevel and senior management.
4. **Analysis and Production**: In this stage, intelligence assessments are packaged and shared with customers (e.g., executive leadership) to better inform corporate decisions. These intelligence assessments are derived by comparing integrated and evaluated information with known facts and predetermined assumptions. These deductions are combined and assessed to discern patterns, recognize events and discover anomalies. The intelligence assessments produced may culminate in reports such as tactical cyber threat indications and warnings and general intelligence insights (e.g., newly discovered vulnerabilities in commercial software/hardware or the supply chain).

5. **Dissemination**: As the intelligence assessment is finalized, it is reviewed by leadership to ensure it meets the initial requirements and the data therein are appropriately classified for dissemination. Recipients could include other analysts, senior executives (technical and nontechnical), and other nontechnical customers. This wide-ranging audience needs to be able to understand the information, digest its content, and understand what action needs to be taken.

6. **Consumption**: Ensuring the intelligence products meet the needs of the customer is essential. Therefore, the provided intelligence needs to be tailored to the key interests and objectives of the different audiences. Each audience should see how the information can affect their business or mission objectives.

7. **Feedback**: Customer feedback is critical to determining whether the product has met its requirements or if follow-up work is needed. Ideally, feedback is performed continuously throughout the lifecycle. Cyber intelligence planners, collectors, analysts, and disseminators coordinate to determine whether any of the operations require improvements. Intelligence operators aggressively seek to improve their own performance and the performance of the team activities in which they participate.

Certain information — such as precise, real-time attack indicators — demands immediate action, while, for instance, general knowledge of advanced persistent threats (APTs) targeting similar organizations requires awareness and incorporation into longer-term defensive initiatives. A cyber threat intelligence process must be able to accommodate both, supporting not only day-to-day security operations but also informing the organization's long-term strategic outlook.
INFORMATION SHARING

No matter how rigorous and prescient an organization’s cyber intelligence lifecycle may be, it cannot succeed in a vacuum. Successful sharing of data, insights and analytics is integral to an effective tactical cyber intelligence program. The combined knowledge and timely collaboration of many organizations strengthens the security posture of all involved. Currently, cyber threat information sharing is conducted most visibly on a sector-specific basis through the Information Sharing & Analysis Centers. Through ISACs, organizations can share technical and nontechnical data consistently and effectively. Many ISACs are dedicated to critical infrastructure, including electricity, water, public transit and financial services.

Recently, the U.S. government has made notable strides to foster cyber threat information sharing with the private sector at large. In February 2015, President Obama signed an executive order, *Promoting Private Sector Cyber Security Information Sharing*, “to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government.” The order also directed establishment of the National Cybersecurity and Communications Integration Center (NCCIC) to serve as “the 24/7 hub for cybersecurity information sharing, incident response and coordination across the federal government and with private sector partners.”

The executive order also addressed a significant challenge to information sharing, which has been the lack of uniformity across information sharing processes. The University of Texas at San Antonio has been named the Standards Organization for the development of Information Sharing & Analysis Organizations (ISAOs), which would allow for more cross-sector information sharing, according to the Department of Homeland Security:

> Through public, open-ended engagements, the ISAO Standards Organization will develop transparent best practices that align with the needs of all industry groups, not just those traditionally represented by ISACs. Although membership and operations standards will be developed by the Standards Organization, the ISAO best practice models are intended to be:

- **Inclusive** – Groups from any and all sectors, non-profit or for-profit, expert or novice, should be able to participate in an ISAO.
- **Actionable** – Groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO.
- **Transparent** – Groups interested in an ISAO model will have adequate understanding of how that model operates and if it meets their needs.
- **Trusted** – Participants in an ISAO can request that their information be treated as Protected Critical Infrastructure Information (PCII). Such information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation.
As more organizations begin to share technical data in real time, a number of prerequisites have emerged that will need to be met to optimize efficiency and effectiveness.

1. **A common cyber threat data taxonomy and vocabulary.**
   The MITRE-developed Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) are potential tools to help an organization begin to “speak the same language” as other public and private sector organizations participating in cyber threat data sharing. STIX is a structured language for describing cyber threat information so it can be shared, stored and analyzed in a consistent manner. TAXII is “the main transport mechanism for cyber threat information represented in STIX.” When implemented, TAXII enables sharing of actionable cyber threat information across organizations and product/service boundaries. TAXII also defines concepts, protocols, and message exchanges to share cyber threat information for the detection, prevention, and mitigation of cyber threats.

2. **An approach for receiving, searching, analyzing, and storing cyber threat data.**
   Organizations cannot effectively share information without the ability to receive and store it as well. If an organization does not have the wherewithal to internally develop this capability, it can be accomplished by either investing in a commercial platform or contracting it as a service to an outside vendor. The growth of cyber intelligence as a security priority has produced a competitive marketplace offering these platforms and services.

3. **The capability to automate the sharing of cyber threat data.**
   Given the evolving complexities of the threat landscape, the speed at which events occur, and the vast quantities of data involved in cyber intelligence and in cyber threat information sharing, driving effective automation to aid human analysis or execute defensive actions at machine-speed is a prerequisite for any effective approach. By utilizing TAXII or a similar mechanism, organizations can share cyber threat information in a secure and automated manner.

4. **The ability to incorporate human analytic judgment whenever feasible.**
   In many cases, organizations have a desire to exchange information in a way that is both human-readable as well as machine-parsable. Organizations consume not just the data but also assess the data as part of an intelligence collection and analysis process. There is no precise substitute for human analytic judgment in assessing the value of a particular piece of intelligence.

5. **An understanding of how to classify cyber threat data.**
   Data classification here refers to the broader data management principle rather than the security clearance parlance of the IC. Classifying data can maximize sharing while minimizing risk of sources and methods being compromised. A number of ISACs use the Traffic Light Protocol (TLP) to facilitate sharing of information. It uses the familiar color scheme to provide guidance about how widely the data should be shared and how those recipients should leverage it (see page 11). When receiving a document that is TLP Amber, an organization’s cyber intelligence professional knows that the sharing of this information is limited to only those who need to know this information. By using TLP or a similar data classification scheme, an organization can ensure that its data will be shared with the appropriate audience, but not so widely that sharing will present risks to its security or reputation.
CYBER THREAT DATA FEEDS

Information sharing is an asset only if the information shared offers value, making quality sources of internal and external cyber threat data a key element of a tactical cyber intelligence program. Finding valuable data sources is often predicated upon knowing what data sets you have and what insights you need. The goal is to develop multiple sources that can provide a comprehensive understanding of threats your sector is facing, which threat vectors your organization is most vulnerable to, and how you can prevent or detect the activity. In a best-case scenario, these feeds can help organizations identify adversaries and their objectives.

The cyber intelligence team should consider not only the attributes of the threat feed but also the organization’s ability to make use of the data.

The cyber intelligence team should consider not only the attributes of the threat feed but also the organization’s ability to make use of the data. Having a firehose of data is only helpful if you are able to intake, process and manage this information to gain important insights. Acquiring key information requires having a clear view about the needs of the organization, knowing what data feeds work best and having the right methodology to make the most of it.

Based on current knowledge of the organization’s security posture and identified points of entry, the cyber intelligence team needs to determine what additional data would help prevent, detect, or predict attacks. For instance, there may be a surge of spear phishing emails affecting one of the business units and the team wants to know if and when other units could get hit. Additionally, an ISAC may identify a specific type of attack targeting certain technologies. The organization can use this data to identify clear areas of vulnerability that need to be shored up.

Relationships with colleagues inside and outside the organization, peers at other companies, industry experts and associations, and local law enforcement and government officials can provide useful sources of information and cyber intelligence.

Sources of Threat Data

GOVERNMENT SOURCES:
Law enforcement, government agencies, computer emergency response agencies

INDUSTRY ASSOCIATIONS AND NETWORKS:
Security researchers, peers at other companies, informal information sharing groups or associations

COMMERCIAL SOURCES:
Threat intelligence research services, threat feeds

EXTENDED ENTERPRISE SOURCES:
Managed security service providers, business partners

INTERNAL SOURCES:
Employees, contractors, executives, IT and security infrastructure

PUBLIC SOURCES:
Internet (social media, Web sites, message boards, webinars, etc.), conferences and forums
In order to evaluate sources of cyber threat data, some criteria include:

- How trustworthy is the source?
- Is the data provided by this source actionable?
- If the source is derived from our internal IT infrastructure, do we have the right tools to capture or generate the right data?
- Do we have the time to invest in fostering the relationships that may be required to leverage this data source?
- What are the costs involved?
- If it is an information-sharing arrangement, are the required processes in place? Are we clear on what data we share?

Traffic Light Protocol

**RED**
**WHEN SHOULD IT BE USED?**
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party’s privacy, reputation, or operations if misused.

**RED**
**HOW MAY IT BE SHARED?**
Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

**AMBER**
**WHEN SHOULD IT BE USED?**
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

**AMBER**
**HOW MAY IT BE SHARED?**
Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.

**GREEN**
**WHEN SHOULD IT BE USED?**
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.

**GREEN**
**HOW MAY IT BE SHARED?**
Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

**WHITE**
**WHEN SHOULD IT BE USED?**
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

**WHITE**
**HOW MAY IT BE SHARED?**
TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Figure derived from www.us-cert.gov/tlp.
CONCLUSION

Primarily inward-focused cybersecurity approaches are not independently sufficient against today’s cyber threat landscape. Just as locks and alarms are needed for physical security, you also need to know the crime trends and daily events in your neighborhood, so that you can take measures to protect your family or business. There is a comparable need for more outward-looking and collaborative approaches in cybersecurity. Tactical cyber intelligence enables organizations to identify and minimize potential threats and vulnerabilities, and gives adversaries less time to operate on a network before they are discovered. Internally, it helps organizations understand what they have, where the risks reside, and how to strengthen and mature their security architecture.

The value proposition for a cyber intelligence program includes insight into your sector’s operating environment, the ability to prevent a majority of cyber adversaries from disrupting your network or stealing your data, and the ability to protect your revenue, mission and reputation in a cost-effective way. Defensive strategies can be put in place and precisely aimed at addressing the most significant threats and protecting the most critical assets. The security team will have the knowledge necessary to make informed risk decisions and invest in the optimal security controls.

Tactical cyber intelligence consists of setting priority requirements, collecting or accessing and analyzing key data, turning the results into a consumable and actionable product and evaluating the usefulness of that product. This then feeds back into asking focused and impactful questions for the future.

Successful integration of tactical cyber intelligence into any organization should contain a basic roadmap detailing the systems you plan to protect, the intelligence techniques you plan to implement, the capabilities that you plan to develop, and the timeframes of when each technique will be implemented. Information sources should be identified, aggregated, and validated; they also should provide data related to the types of threats that present the greatest risk.

Tactical cyber intelligence is complementary to, but does not replace, an organization’s traditional cybersecurity technologies and approaches. Striking a balance between the two, and allowing the former to strengthen the latter, is the best path forward to stay ahead of adversaries targeting your organization or its sector.
ENDNOTES


ABOUT THE INSA CYBER INTELLIGENCE TASK FORCE

The INSA Cyber Intelligence Task Force consists of individuals from government, the private sector and academia with an interest in promoting the discipline of cyber intelligence as an emerging yet essential component of cybersecurity practices. The Task Force is chaired by John Felker, director of operations for the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security and Geoff Hancock, CEO of Advanced Cybersecurity Group. Since 2011, the Task Force has published white papers on the strategic, operational and tactical value of cyber intelligence to organizations from the public, private, nonprofit and academic sectors.

ABOUT INSA

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

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