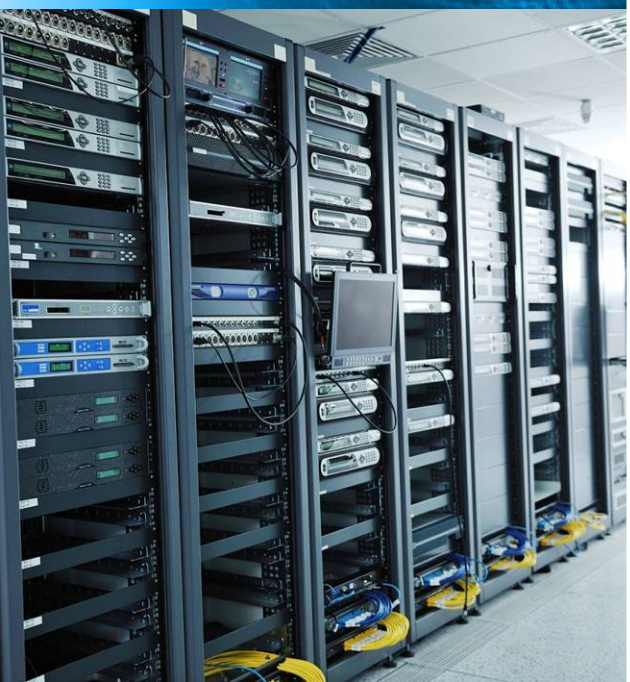


Cyber Network Guide Studies in Systems, Decision and Control

By Fiedelholtz
UMBC Professor

This page intentionally left blank.

Table of Contents

Figures

Appendix

Acknowledgements

I would like to dedicate this cyber book to Jennifer Fiedelholtz, who has stood by me with all my crazy career changes and who gave me two beautiful children, Sarah and Matthew.

In addition, this Cyber Network book would not be possible if not for the tireless efforts of the team at *Media Graphics Lab*, Rockville, Maryland. The excellent graphic diagrams in this book is a reflection of their graphics skills and command of the computer science principles encapsulated in this material.

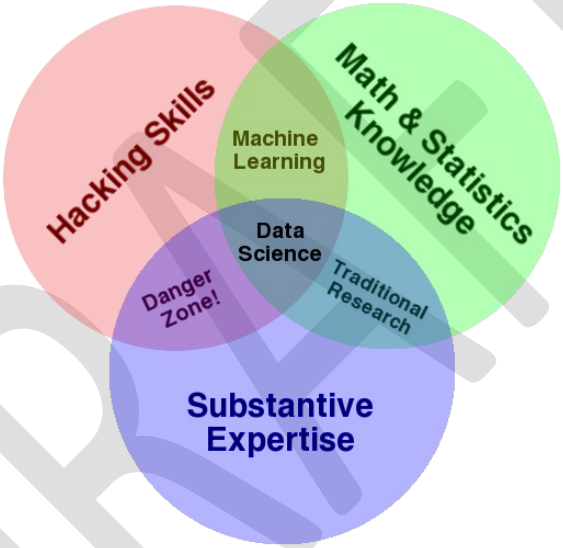
Finally, while teaching at University of Maryland at Baltimore (UMBC), I noticed that a more hands-on approach to supplement their excellent computer science pedagogical foundational approach is needed. This cyber book will address that gap to provide the university with both a computer science comprehensive theoretical and hands-on skills.

Abstract

1 Pre-incident Planning and Analysis

The purpose of cyber-physical planning and analysis under the Cyber Network Guide, Studies in Systems, Decision and Control textbook is to standardize requirements for cyber-physical preparedness (**including vulnerability and consequence analysis**) and operational incident response for all international cyber stakeholders.

2 Incident Detection and Characterization



The Cyber Operation Centers will continue to serve as a centralized location where operational elements involved in cybersecurity and communications dependence are coordinated and integrated. The cyber incident response partners include all Federal departments and agencies; State, local, tribal, and territorial governments; the private sector; and international partners. In close coordination with the originators of information and with other partners, the Federal requests, receives, shares, and analyzes information on cyber-attack techniques and vulnerabilities from the range of the highest to the lowest level of classification or restriction possible and works with Federal partners to mitigate threats to critical networks.

In this process, the Federal government continues as the information and coordination hub of a national network to protect critical infrastructure. Specific Federal government roles include situational awareness and crisis monitoring of critical infrastructure, and information sharing on threat information and collaboration, assessment and analysis, and decision support pre- and post-incident.

Both the Federal government and private sector will assist and collaborate sector analysts and provide actionable information in real time for comprehensive cyber and physical analysis of critical

infrastructure during an incident (manmade and/or natural disaster). The centers' activities include analysis and providing a greater situational awareness of cybersecurity and communications vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

3 Vulnerability/Consequence Analysis

3.1 Information Sharing

Secure, functioning, and resilient critical networks requires the efficient exchange of information, including intelligence, between all levels of government and critical infrastructure sector owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents.

To conduct vulnerability/consequence analysis of any particular sector or potential exploit, the analyst will collect relevant data from cyber operational centers on credible cyber threats and combine it with cyber-physical system information from owner/operators. Collection of data includes understanding potential cyber exploit details, potential impacts on the entity based on their information, and relevant mitigation steps. The analyst will leverage partnerships with the government, industry, and international partners to determine risk to infrastructure owners and operators from credible cyber threats. These analyses will provide the basis for pre-incident preparedness activities and post-incident response and recovery.

4 Incident Response and Recovery

The cyber analyst in the cyber-physical response and recovery will provide necessary support in the analysis and development of response and recovery action plans to protect the sector entity or infrastructure property, business needs, and the environment after an incident has occurred and then continue this effort in stabilizing the incident. Response and recovery efforts are focused on ensuring that the sector entity or infrastructure is able to effectively respond to any threats with an emphasis on economy, environment, and safety.

The ensuing recovery process includes those capabilities necessary to assist the sector entity or infrastructure asset, as well as communities affected by an incident, in recovering effectively and prioritizing action plans and support. It is focused on timely restoration, strengthening, and revitalization of the infrastructure. Successful recovery requires informed and coordinated leadership, collaboration between the sector partners during all phases of the recovery process.

5 Cloud Architecture

Cloud Computing is currently an essential part of network infrastructure. The U.S. National Institute for Standards and Technology has proposed defining cloud computing as a model "for enabling convenient, on-demand network access to a shared pool of configurable computing resources." The cloud structure facilitates the user to access the real-time metadata in a quick and more efficient manner. Data uploads into a centralized data center and is distributed through the network in milliseconds.

6 Lessons Learned

Once the cyber-physical analysis and incident response and recovery action and plans are communicated to the sectors or entities in question, the cyber operational agencies, sector agencies, and the sector or

entity involved should review the entire incident analysis process to determine what worked and identify areas of weakness to improve the process for the next incident response and recovery analysis.

The lessons learned process should strive to identify shortcomings of the process that walks through the D Cyber-Physical Mapping Framework Analysis Process Matrix depicted in Appendix F (i.e., pre-incident planning and analysis, incident detection and characterization, vulnerability/consequence analysis, incident response and recovery, roles, responsibilities, collaboration, support, various report outputs, and training). The lessons learned should provide guidance for the additional need for training for all the personnel involved in the cyber-physical incident analysis.

The lessons learned should also focus on collecting data, sharing information, providing guidance and assisting the sector or entity in preventing future attacks, preventing or limiting disruption if they do occur, and creating early visibility of such attacks through enhanced awareness, security monitoring, and training.

Preface

The Cyber Network Guide, *Studies in Systems, Decision and Control* textbook provides a cybersecurity technical foundational landscape of the international government cyber operational capabilities for college undergraduate and graduate students, which includes standard operating procedures, cyber operational documentation, and description of tools utilized in the event of a major cyber incident.

The cyber textbook provides in-depth background information for each step of the cyber analytic framework process, which includes the following requirements:

- Pre-incident planning and analysis
- Incident detection and characterization
- Vulnerability/Consequence analysis
- Incident Response and Recovery
- Cloud Architecture Analysis

The purpose of the Cyber Network Guide, Studies in Systems, Decision and Control book is to standardize requirements for cyber-physical international operational analysts and response for cyber practitioners.

This unique technical guide provides Cyber Analysts with appropriate *Open Source* background information to underpin efforts to provide accurate and comprehensive inputs in the development of cyber analytic products. In addition, this cyber primer is an effort to provide cyber baseline information in collaboration with international governments regarding vulnerability and consequence analysis for responding to cyber network attacks

This page intentionally left blank.

1 Pre-incident Planning and Analysis

The purpose of cyber-physical planning and analysis under the Cyber Network Guide, Studies in Systems, Decision and Control textbook is to standardize requirements for cyber-physical preparedness (**including vulnerability and consequence analysis**) and operational incident response for all international cyber stakeholders.

1.1 Steady-state and Continuous Monitoring

The cyber and private sector international organizations under this cyber-physical incident process and monitoring will, in advance, have the mechanisms and facility to allow the development of a common operational picture of the incident in question based on participation and input. Preparation also includes training to ensure individuals, teams, and organization leadership are trained in cyber-incident response procedures and internal/external reporting mechanisms. Training should also ensure that individuals meet professional qualifications and performance standards and have been trained in their specific cyber roles within their organization structure and process.

During steady-state and monitoring activity, the international cyber organizations will leverage expertise in working with the international cyber governments and private sector organizations to identify critical areas for vulnerability and consequence analysis as it relates to infrastructure dependency, interdependency, cascading effects, and cross-sector impacts of a potential incident. Cyber analysts will collaborate to standardize understanding of roles and responsibilities among the partners (Figure 1). Each organization plays a unique role in preparing for a cyber incident with respect to its distinct mission and organizational authorities.

In the context of the United States National Infrastructure Protection Plan (NIPP), “steady state” is defined as the posture for routine, normal, day-to-day operations, as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. Activities completed by the international cyber analysts during the steady-state period include the following:

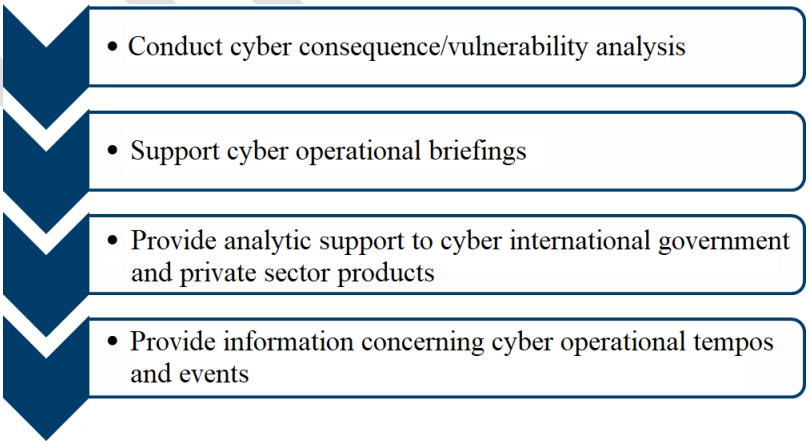


Figure 1 Cyber Incident Standard Operating Procedure (SOP)

For roles, responsibilities, and processes in the cyber-physical incident planning and response framework, the cyber analysts should refer to the most recent Gartner report referencing cyber-attacks and disruption of business activities.[1]

[1] "How to Prepare for and Response to Business Disruption After Aggressive Cyber Attacks", August 2019

2 Incident Detection and Characterization

The Cyber Operation Centers will continue to serve as a centralized location where operational elements involved in cybersecurity and communications dependence are coordinated and integrated. The cyber incident response partners include all Federal departments and agencies; State, local, tribal, and territorial governments; the private sector; and international partners. In close coordination with the originators of information and with other partners, the Federal requests, receives, shares, and analyzes information on cyber-attack techniques and vulnerabilities from the range of the highest to the lowest level of classification or restriction possible and works with Federal partners to mitigate threats to critical networks.

In this process, the Federal government continues as the information and coordination hub of a national network to protect critical infrastructure. Specific Federal government roles include situational awareness and crisis monitoring of critical infrastructure, and information sharing on threat information and collaboration, assessment and analysis, and decision support pre- and post-incident.

Both the Federal government and private sector will assist and collaborate sector analysts and provide actionable information in real time for comprehensive cyber and physical analysis of critical infrastructure during an incident (manmade and/or natural disaster). The centers' activities include analysis and providing a greater situational awareness of cybersecurity and communications vulnerabilities, intrusions, incidents, mitigation, and recovery actions.[2]

2.1 Detection

When prevention and protection efforts are unsuccessful, Federal, State, local, tribal, territorial, and private-sector owners and operators of critical networks and infrastructure are likely to be the first to detect malicious or unauthorized activity on their networks. In general, the critical infrastructure sector owners and operators work independently and within their company's incident response processes to address cybersecurity issues. These private-sector owners and operators in partnership with others, when appropriate, identify and contain malicious and unauthorized activity on their critical networks (from internal/external cyber attacks). They seek to gather as much information as possible on the unauthorized activity, including any critical details on the "who, what, where, when, why, and how" of the incident, if known. As part of this activity, organizations reporting an incident may report directly to the Federal Operation Centers through its collocated organizations; indirectly through the Situation Operation Center (SOC), National Operation Center (NOC), or law enforcement, intelligence, and regulatory agencies; indirectly through Information Sharing and Analysis Centers (ISACs); and/or directly from the private sector.[3] Activities related to detection conducted by the Cyber Analyst in collaboration with Federal Cyber Operation Centers may include the following:

- **Conduct open source monitoring** – Monitor the Cyber Daily Open Source Infrastructure Report, a summary of open-source published information collected each business day concerning significant critical cyber issues. Each Daily Report is divided by critical infrastructure sectors and

[2] DHS, undated a, " Cybersecurity and Infrastucture Agency (CISA), 2019,us-cert.gov/NCCIC Reports/year-in-Review_Final_5500BC.pdf

[3] DHS, 2019, "Bottom-Up Review Report," ics-cert us-cert.gov/sites/default/files/Annual

key assets defined in the NIPP, and discusses relevant physical and cyber incidents across the Nation.[4]

- **Collect datasets (security incidents, alerts, and events)** – During the cyber incident, review and collect, major cyber reports, as well as sector reports of essential security incidents, alerts, events, and information on control systems in sector area(s) of concern. Such reports may include the Suspicious Activity Report (SAR), U.S. Computer Emergency Readiness Team (US-CERT), and Industrial Control System-Computer Emergency Readiness Team (ICS-CERT) weekly and monthly reports; Open Source Infrastructure report and analysis; and others.

- **Identify and analyze suspicious activity** – Identify and analyze suspicious activity reporting (SAR) from the Nationwide Suspicious Activity Reporting Initiative (NSI) database. The SAR initiative is a collaborative effort led by the U.S. Department of Justice (DOJ), Bureau of Justice Assistance, in partnership with the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and State, local, tribal, and territorial law enforcement partners. The program establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information among law enforcement agencies. SAR reports are vetted by the cyber fusion centers and shared as appropriate among NSI participants.

- **Detect and verify unusual and network traffic** – Cyber Operation Centers, will review, detect, and verify real-time cyber data with automatic collection tools, and conduct deep packet inspection of traffic coming to or from Federal Internet protocol (IP) addresses ending in ".com" or ".gov" to detect signs of suspicious or malicious activities.

- **Review and collect sector reports of essential information systems** – Review and collect relevant critical infrastructure sector reports and information through existing partnership agreements with critical infrastructure owners/operators, Federal agencies, and State/local governments:

  - **Critical infrastructure owners/operators** – Through their collaborative agreement with the critical infrastructure sector owners and operators will coordinate and communicate directly with the appropriate leadership of critical infrastructure owners/operators. This may include crucial communication with the Multiple Sharing and Analysis Center (ISACs) during a cyber incident.

  - **Federal agencies** – Significant cyber incidents may require nationally-coordinated rapid response actions based on differing authorities and priorities. Numerous organizations may provide essential data and capabilities: DHS, National Security Agency (NSA), DOJ, FBI, Department of State, and other Federal departments and agencies.

  - **State and local government** – Personnel from State, local, tribal, or territorial governments also play a major role in providing relevant information about the sector or entities, through media such as the Multi-State Information Sharing and Analysis Center (MS-ISAC).

- **Einstein 1, 2,** – Review the Einstein situational awareness report when studying the cyber incident. Einstein 1, and 2 is a program launched by the National Cyber Security Division (NCSD) in 2004. It is a phased program that adds new functionality to combat cybersecurity

[4] DHS, 2013, "DHS Daily Open Source Infrastructure Report," available at http://www.dhs.gov/dhs-daily-open-source-infrastructure-report, accessed March 25, 2013.

exploits to Federal executive agency information technology (IT) enterprises. The first phase, Einstein 1, an intrusion detection system (IDS), was designed to provide situational awareness for civilian agencies by collecting computer network security information such as network flow records, source IP address, port address, communication time, destination IP address, and the port of the computer. Einstein 2, launched in 2008, incorporates network intrusion detection that monitors for malicious activity in the network traffic to and from participating Federal executive agencies.

- **Intelligence analysis** – The purpose of intelligence analysis is to reveal the underlying significance of selected incident information. The Federal government should begin with confirmed and verified incident information based on data source such as the NSA, Central Intelligence Agency, or FBI, and apply expert knowledge to produce plausible data for the initial briefing, final briefing, and reports to the stakeholders.

- **Review updates** – The collection of data and appropriate cyber-incident information from the various internal and public sources, Federal partners, and sector entities listed will be continually revisited and updated as appropriate by the cyber analyst to better assess the risks and consequences from the cyber attack.

2.2 Threat Analysis

Cyber threat analysis is the practice of effectively fusing incident information, knowledge of an organization's network and vulnerabilities—both internal and external, including essential IT and industrial control systems (ICS)—and matching these against other actual cyber attacks and threats that have been observed or reported. The output of this fused analysis is an advanced defensive detection mechanism with a final goal of enhancing the defensive posture of seemingly unaffected or affected asset owners of the critical infrastructure network.

As part of this process, the cyber analysts are responsible for threat analysis, which will characterize the attack, including scope and scale, from forensic information, and will attempt to ascertain the level of sophistication of the attack and the potential impact to the sector(s). This will include identification of other potentially vulnerable sector(s) and possible detection mechanisms for the attack. The attack's level of severity will be based on the seven layers of the Open Systems Interconnection (OSI) Model. The steps for threat analysis are as follows:

- **Identify tactics, techniques, and procedures (TTPs)** – The cyber analyst identifies tactics, techniques, and procedures that pertains to cyber attacks. Attacks such as distributed denial of service (DDoS), Internet of Things (IOT) and Ransomware are just few examples that the critical infrastructure sectors operators may experience in the year 2019. For more details on the top 10 types of attacks, see Appendix B.

- **Define scope/scale** – The Federal government should identify the scope and scale of the cyber-physical incident in terms of the interruption of the continuity of daily business activities.

- **Determine the intent and capabilities** – The cyber analyst may seek information from operation centers on the intent, scale, and capabilities of the cyber attack (if available) to determine the type of attack and to understand the impact the disruption will have on the critical infrastructure and the potential defense and detection mechanisms that will be required for mitigation.

- **Identify the sector affected (16 sectors) and any additional sector(s) with the potential to be affected** – The analyst should identify the sector(s) affected by the cyber-physical exploit to understand the upstream and downstream disruption impact on the sector supply chain and other sector(s) dependencies. This should include identification of other sectors that may be similarly vulnerable, so that the appropriate notification can be developed and communicated.

  - **Identify systems affected: cyber or physical** – To understand the impact of a cyber-physical exploit on network infrastructure, it is imperative that information and control systems of the affected infrastructure be identified and understood by the analyst in terms of cyber-physical operational vulnerabilities and consequences.

  - **Determine severity** – Review seven layers of the OSI Reference Model to understand the severity of the cyber attack on the network systems, the cyber analyst should review the seven layers of the OSI Reference Model as a guide for how data are transmitted over the network. The OSI Reference Model is a representation of the critical data pathway that an adversary can exploit.

- **Identify and review forensics (Infrastructure Protection Packet Capture, Security Information and Event Management [SIEM] Forensic Integration Tool)** – The most common goal of performing network forensics or digital media analysis is to gain a better understanding of an event of interest by finding and analyzing the facts related to that event. Forensics may be needed in many different situations, such as evidence collection for legal proceedings and internal disciplinary actions, and handling of malware incidents and unusual operational problems. See Appendix A for additional cyber incident analysis tools.

  Computer and network forensics, or digital media analysis, has evolved to assure proper representation of computer crime evidentiary data in court. National Institute of Standards and Technology (NIST) SP800-86, *Guide to Integrating Forensic Techniques into Incident Response*, describes the forensic or digital media analysis process in terms of collection, examination, analysis, and reporting (Figure 2).

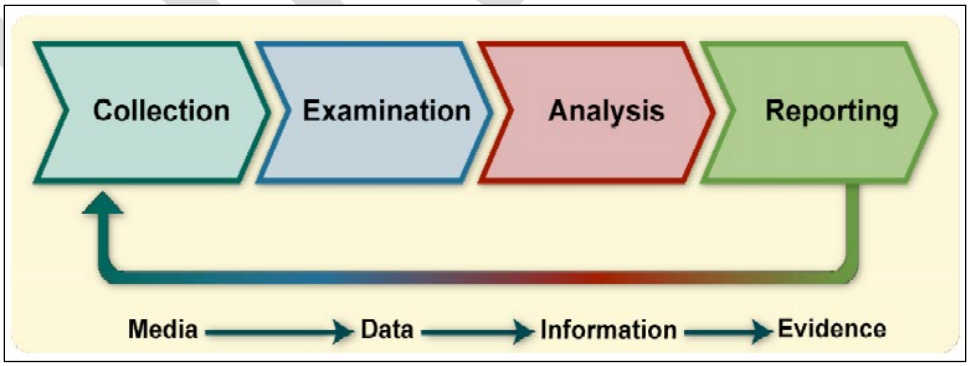


Figure 2 Cyber Digital Media Analysis Process[5]

[5] Kent, K., S. Chevalier, T. Grance, and H. Dang, 2006, "Special Publication SP800-86, Guide to Integrating Forensic Techniques into Incident Response," *NIST*, August, available at http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, accessed March 25, 2013.

Digital media analysis data using tools and techniques such as the IDS Network Forensic Analysis Tool (NFAT) and SIEM provide incident logs and traces that are useful in determining the type of attack and criminal behavior. Forensics or digital media analysis are most often thought of in the context of criminal investigations and computer security incident handling used to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event. Many forensic or digital media analysis tools and techniques can be applied to troubleshooting operational issues, such as finding the virtual and physical location of a host with an incorrect network configuration, resolving a functional problem with an application, and recording and reviewing the current operating system (OS) and application configuration settings for a host. Tools and techniques are available to analyze log entries and recover lost data from user and host systems. NIST SP800-86 provides a guide to integrating forensic or digital media analysis techniques into incident response.[6]

- **Review and identify network configuration vulnerabilities (e.g., sensors, firewalls, routers, host, IDS/intrusion protection system [IPS], host anti-virus [AV])** – The cyber analysts should consider reviewing and identifying critical network vulnerabilities during the initial stage of the cyber-incident analysis (if available); these may include misconfigured firewalls, sensors, routers, IDSs and IPSs, and host AV software, as well as risks associated with vendor-supplied software, risks associated with the network, and systems administration errors. If the information is not available in the initial analysis, efforts should be made to seek this information during a latter stage of an analysis, such as digital media analysis, to aid in the development of response and recovery plans. The following are other vulnerabilities that should be considered:

  - *Network vulnerabilities* – Review of network vulnerabilities across information and control systems includes computers, network hardware/systems, OSs, and software applications that may have originated from a vendor system, system administration activities, and/or user activities.

  - *Vendor vulnerabilities* – Vendor-originated vulnerabilities includes software bugs, missing OS patches, vulnerable services, insecure default configurations, and Web applications.

  - *System administration vulnerabilities* – System administration originated vulnerabilities include incorrect or unauthorized system configuration changes and lack of password-protection policies.

  - *User vulnerabilities* – User-originated vulnerabilities include sharing of directories with unauthorized users, failure to run virus scanning software, and malicious activities such as introducing system backdoors.[7]

- **Review network control systems-**Through the Cyber Operation Centers, the analyst leverages capabilities that provide onsite support and mitigation information for protection against and in response to cyber threats; such information may include incident response, forensic analysis, and site assessments. Information and data from ICS-CERT investigative, forensic, or digital media analysis tools can provide situational awareness of evolving threats to an ICS from cyber exploits.

[6] Kent, K., S. Chevalier, T. Grance, and H. Dang, 2006, "Special Publication SP800-86, Guide to Integrating Forensic Techniques into Incident Response," *NIST*, August, available at http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, accessed March 25, 2013.

[7] How to Scan Backdoors of Your Hacked Word Press by Sufie Banu, June 5, 2018

For example, during the discovery of Stuxnet malware, the network analysis quickly revealed that sophisticated malware of this type potentially has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes.

- **Filter information through the Cyber Operation Centers** – The cyber analyst should filter the incident and its impact to the sector entity in close cooperation with the different cyber entities. The operational centers continuously monitor national and international incidents and events that may affect emergency communications.

2.3 Malware Analysis

Malware analysis entails comprehensive review of the regional risk from an infrastructure disruption from cyber threats (see Appendix B). The analysis provides a holistic view of the problem to assist the critical sector(s) in response and recovery. The analysis should consider the following:

- **Collect and analyze the data profile** – Collection and analysis of data should include information needed to analyze and manage critical infrastructure risks. The dataset should include addresses, points-of-contact, asset geo-location, and other information. This data should leverage geographic information system to visually represent the data on a map; it can be sorted by sector, risk, and priority. Output should provide tabular results of the critical infrastructure in question.

- **Perform security and vulnerability assessments** – This step should provide analysts a way to assess the vulnerabilities and consequences of the threat's impact on infrastructure assets. Current cyber threat modeling and analysis tools should provide a comprehensive score based on past and current analyst knowledge and experience. The assessment should allow the analyst to tweak data based on local threat and sector conditions.

- **Separate asset groups for analysis and monitoring** – The malware analysis should allow the analyst to separate and prioritize asset groups based on threat and consequence. These sector assets can be efficiently monitored for manipulation of data based on changing conditions in the field.

- **Document and disseminate results** – The analyst can document the results from the malware analysis and target the results based on a specific audience and according to the different protocols.

2.4 Cyber Incident Threat Information Process

The cyber analyst can seek information from various cyber threat models, which may include threat identification, characterization, and indicator patterns for detection and investigation of specific incidents, in order to determine reactive courses of action. These models are utilized as a structured language for cyber threat intelligence information that capture, characterization, and communication of standardized cyber-threat information; it improves consistency, efficiency, interoperability, and overall situational awareness. A variety of high-level cybersecurity cases rely on such information (Figure 3), which is provided by cyber analysis, which works in conjunction with Common Indicator Threat Information . See Appendix C for more information on cyber analysis processes. Analytic components to consider in this process include:

- **Analyzing cyber threats** – A cyber threat analyst reviews structured and unstructured information regarding cyber threat activity from a variety of manual or automated input sources.

The analyst seeks to understand the nature of relevant threats, identify them, and fully characterize them such that all of the relevant knowledge of the threat can be fully expressed and evolved over time. This relevant knowledge includes threat-related actions, behaviors, capabilities, intents, attributed actors, and other information.

- **Specifying indicator patterns for cyber threat** – A cyber threat analyst specifies measurable patterns that represent the observable characteristics of specific cyber threats, as well as their threat context and relevant metadata for interpreting, handling, and applying the pattern and its matching results.

  For example, in the case of a confirmed phishing attack, an analyst may harvest the relevant set of observables (e.g., to or from addresses, actual source, subject, embedded uniform resource locators [URLs], type of attachments, specific attachment) from the performed analysis of the phishing email, identify the relevant TTPs exhibited in the phishing attack, perform a kill-chain correlation of the attack, assign appropriate confidence for the indicator, determine appropriate handling guidance, generate any relevant automated rule patterns for the indicator (e.g., Snort, OVAL), assign any suggested courses of action, and package it as a coherent record for sharing.

- **Managing cyber threat response activities** – Cyber decision-makers and cyber operations personnel work together to prevent or detect cyber threat activity and to investigate and respond to any detected incidences of such activity. Preventative courses of action may be remedial in nature to mitigate vulnerabilities, weaknesses, or misconfigurations that may be targets of exploit. After detection and investigation of specific incidents, reactive courses of action may be pursued. For example, in the case of a confirmed phishing attack with defined indicators, decision-makers and personnel work together to fully understand the effects of the phishing attack within the environment, including malware installed or malware executed; to assess the cost and efficacy of potential courses of action; and to implement appropriate preventative or detective courses of action.

- **Sharing cyber threat information** – Cyber decision-makers establish policy for what sorts of cyber threat information will be shared with which other parties and how such information should be handled based on agreed-to frameworks of trust to maintain appropriate levels of consistency, context, and control. This policy is then implemented to share the appropriate cyber threat indicators and other cyber threat information. For example, in the case of a confirmed phishing attack with defined indicators, the policies predefined by cyber decision-makers could allow the relevant indicators to be automatically or manually shared with trusted partners or communities so they could take advantage of the knowledge gained by the sharing organization.[8]

[8] The MITRE Corporation, 2018, mitre.org>capabilities>cybersecurity>cyberthreat intelligence

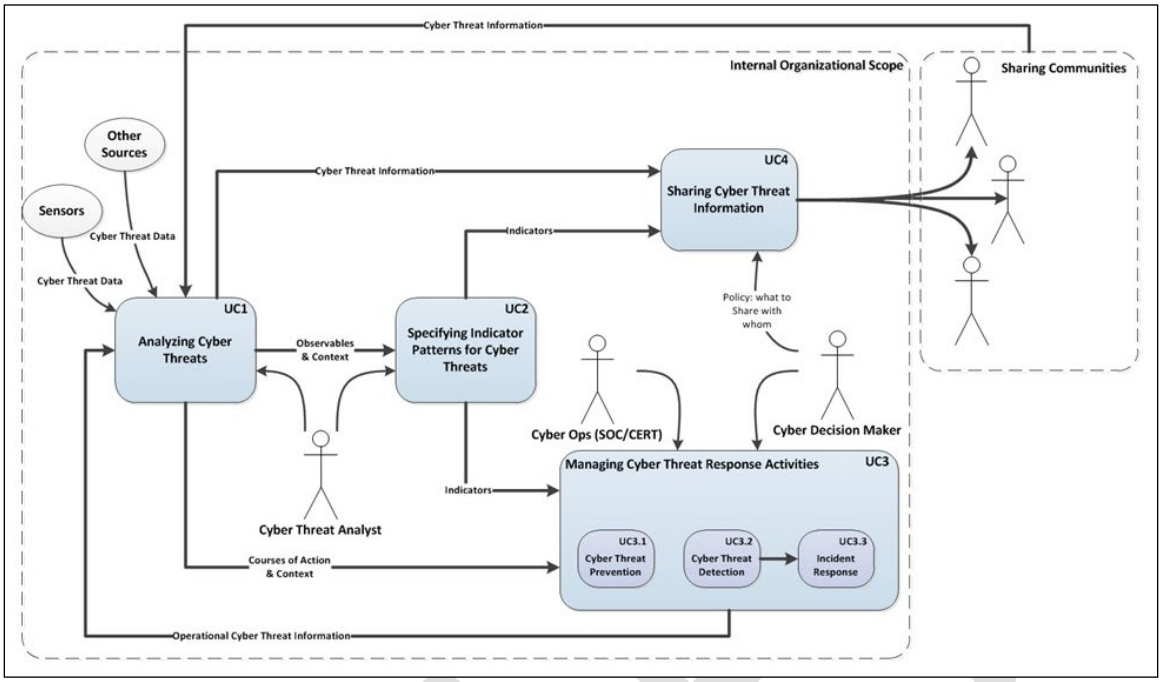


Figure 3 Notional Core Use Cases Targeted by Cyber Indicators™[9]

[9] https://stix.mitre.org