How Do You Assess Your Organization's Cyber Threat Level?

Deb Bodeau, Jenn Fabius-Greene, and Rich Graubart
The MITRE Corporation

Abstract: In the Cyber Prep methodology, an organization determines its target level of preparedness against cyber threats, including the advanced persistent threat, based on its assessment of the level of the adversary it faces. That is, an organization calibrates its cyber security measures, as well as its cyber security governance, to its cyber threat. Cyber Prep characterizes the cyber threat in terms of an adversary's level of capability, intent, and targeting. However, many adversaries demonstrate a mixture of levels. Organizations can differ in how they account for such adversaries. Those differences reflect an organization's attitude toward the advanced cyber threat. A set of anchoring examples illustrates how different attitudes can result in different assessments of adversary level.

Introduction

Cyber Prep is a conceptual framework, together with a practical methodology, which an organization uses to define and implement its strategy for addressing threats related to its dependence on cyberspace.[1] In particular, Cyber Prep enables organizations to articulate their strategies for addressing the cyber threat. The Cyber Prep framework defines five levels of organizational preparedness, characterized in terms of (a) the organization's perspective on, and/or assumptions about, the threat it faces (adversary characteristics and representative threat scenarios), (b) the organization's overall strategy for addressing the cyber threat, in the context of its ICT infrastructure and business processes, and (c) the organization's approach to cyber security governance.

This white paper describes how the Cyber Prep methodology enables an organization to calibrate its target cyber preparedness level to its adversaries – to the cyber threat that it faces. Cyber Prep allows an organization to use a succinct assessment of adversary level. However, some organizations face adversaries with characteristics that do not fit cleanly into a quick characterization or support multiple business or mission functions, each susceptible to different adversaries. Those organizations can use a more nuanced approach which reflects the organization's business or mission environment and its cyber risk tolerance.

The purpose of this paper is to describe alternative approaches to determining the threat level facing an organization. A more complete description of Cyber Prep, including the relationship between the cyber threat level of an adversary an organization's cyber preparedness levels, the tactics, techniques, and procedures (TTPs) the are typical at the various levels, and the safeguards that are needed to counter the TTPs can be found elsewhere [1].

[1] In Cyber Prep, cyberspace is "the collection of information communications and technology (ICT) infrastructures, applications, and devices on which the organization, enterprise, or mission depends, typically including the Internet, telecommunications networks, computer systems, personal devices, and (when networked with other ICT) embedded sensors, processors, and controllers." This definition is designed to be consistent with a variety of existing characterizations [2, 3, 4].

The Cyber Threat

The term "threat" is used in multiple ways. When used in the context of cyberspace, the term typically means one or more of the following:

- A specific adversary or a class of adversaries (e.g., the nation-state threat, the threat of organized crime) which seek to exploit an organization's or a mission's dependence on cyberspace, to achieve specific goals.
- A threat scenario – i.e., a description of how a series of actions or events could exploit an organization's dependence on cyberspace to produce an undesirable outcome (e.g., the threat of system take-over, business loss).
- TTPs (Tactics, Techniques, and Procedures) – methods that an adversary could use in the course of a threat scenario (e.g., the threat of laptop theft).
- The proximate or ultimate source of a threat scenario (e.g., the threat of natural disaster, the threat of human error, the threat of structural failure, the adversarial threat).

In Cyber Prep, the cyber threat to an organization is the *adversary or set of adversaries* – individuals, groups, organizations, or states – that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies). In the Cyber Prep methodology, an organization determines its target level of preparedness against the cyber threat (its target Cyber Prep level) based on its assessment of the level of the adversary it faces. Examples of typical adversaries and their goals at the Cyber Prep levels are given in Table 1.

Table 1. Characteristics of Cyber Threat Levels

Threat Level	Typical Actors	Typical Goals
5: Advanced	Nation-state military possibly supported by their intelligence service; very sophisticated and capable insurgent or terrorist group.	Severely undermine or destroy an organization's mission capabilities by disrupting or denying its use of cyber resources (e.g., information, ICT infrastructure and applications).
4: Significant	Professional intelligence organization or military service operative.	Obtain specific, high value information; undermine or impede critical aspects of a mission, program, or enterprise; or place itself in a position to do so in the future.
3: Moderate	Nation-state government entity; patriotic hacker group; sophisticated terrorist group; professional organized criminal enterprise	Increase knowledge of general infrastructure; plant seeds for future attacks. Obtain or modify specific information and/or disrupt cyber resources, specifically resources associated with missions or even information types.
2: Limited	Individuals or small, loosely affiliated groups; political or ideological activists; terrorists; domestic insiders; industrial espionage; spammers.	Obtain critical information and/or usurp or disrupt the organization's business or mission functions for profit or ideological cause.
1: Unsophisticated	Hackers, Taggers, and "Script Kiddies;" small disaffected groups of the above.	Disrupt and/or embarrass the victimized organization or type of organization (e.g., a specific Department or the Federal government as a whole).

Cyber Prep characterizes levels of the cyber threat in terms of the adversary's

- Capability (resources, skill or expertise, knowledge, and opportunity),
- Intent (goals or outcomes that the adversary seeks; consequences the adversary seeks to avoid; and how strongly the adversary seeks to achieve those outcomes and/or avoid those consequences), and
- Targeting (how broadly or narrowly and how persistently the adversary targets a specific organization, mission, program, or enterprise).

These are presented in Table 2 on the next page.

The Cyber Prep threat characterization intentionally does not limit itself to the more traditional cyber elements (resources, skill, expertise, etc.). Instead it uses an approach similarly employed by intelligence analysts and complements capability with the elements of intent and targeting. This broader based methodology is better suited for Cyber Prep, which takes a strategic, enterprise and national perspective, and is intended to support cyber security investment planning. The Cyber Prep definitions of the cyber threat, and the representation of threat level in terms of capability, intent, and targeting, are intended to be consistent with a variety of sources[2], while remaining true to the strategic and cyber orientation of the Cyber Prep methodology.

How Does Your Organization Assess Adversary Level?

The succinct characterization of adversary levels in Tables 1 and 2 is sufficient for many organizations. When it is not, Cyber Prep accommodates more nuanced assessments. These allow the organization to consider its attitude toward risk factors and toward the temporal aspects of the threat, as well as to address multiple missions or business functions.

Consider Your Organization's Attitude Toward Risk Factors

Organizations can differ in how they account for adversaries whose levels of capability, intent, and targeting are not uniform. Those differences reflect the different organizations' varying attitudes toward how to assess and weight cyber risk factors, in particular the factors related to threats. The following example illustrates how different attitudes can result in different assessments of adversary level. (The appendix to this paper presents a larger set of examples.)

> An extremist group seeks to undermine public confidence in the ability of Government and the private sector to ensure public safety or security, by causing disruption to critical infrastructure systems. The group uses the Internet to conduct initial reconnaissance on prospective target organizations and identifies some candidate target organizations that, if compromised, would allow the group not only to disrupt the services the organizations provide but also to produce ripple effects by damaging the critical infrastructure the organizations support. Based on their knowledge of the candidate targets, the group decides to pursue one particular organization because of its reputation for having cyber security problems, which will allow them to use existing exploits rather than use their limited supply of new ones.

[2] These include the DHS Risk Lexicon [5], the Open Group Risk Taxonomy [6], NIST Special Publication 800-30 [7], the MORDA [8] and NRAT [9] methodologies, the Sandia Threat Analysis Framework [10, 11], and the proposed three levels of cyberaggression (cybercrime, cyberespionage and reconnaissance, and cyber-leveraged war) [12]. Language such as "sophisticated" is intended to be consistent with use in the growing body of publicly available threat reports (e.g., [13]).

Table 2. Adversary Levels

Threat Level	Capability	Intent	Targeting
5: Advanced	The adversary is very sophisticated and well resourced and can generate its own opportunities to support multiple successful, continuous, and coordinated attacks.	The adversary seeks with great determination to undermine, impede severely, or destroy, a mission, program, or enterprise, by exploiting a presence in the organization's systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede their ability to complete their goal.	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, or mission, focusing on specific high value or mission-critical information, resources, supply flows, or functions; specific employees or positions; and supporting infrastructure providers and suppliers and on partnering organizations.
4: Significant	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.	The adversary seeks with determination to undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's systems or infrastructure. The adversary is very concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly while preparing for future attacks.	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, or mission, focusing on specific high value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, and/or key positions.
3: Moderate	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.	The adversary seeks to obtain or modify specific, critical information and/or to usurp or disrupt the organization's cyber resources by establishing a foothold in the organization's systems or infrastructure, but is concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly when carrying out attacks (e.g., exfiltration) over long time periods. The adversary is willing to knowingly impede aspects of the organization's mission to achieve these ends.	The adversary analyzes publicly available information to target persistently specific high value organizations (and key positions, such as Chief Information Officer), programs, or information.
2: Limited	The adversary has limited resources, expertise, and opportunities to support a successful attack.	The adversary actively seeks to obtain critical information and/or to usurp or disrupt the organization's cyber resource, and does so without concern about detection of their attacks or disclosure of tradecraft.	The adversary uses publicly available information to target a class of high value organizations and/or information, and seeks targets of opportunity within that class.
1: Unsophisticated	The adversary has very limited resources, expertise, and opportunities to support a successful attack.	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about detection of their attacks or disclosure of tradecraft.	The adversary may or may not target any specific organization or class of organization.

In this example, the adversary's capability level is three, its intent is five, and its targeting is four. One organization could assess the threat level as five – the maximum of the three components of threat – and thus this adversary could motivate the organization to seek a high level of cyber preparedness. On the other hand, another organization could use the minimum of the three components to assess the threat level – and thus conclude that Cyber Prep level 3 suffices. Cyber Prep does not assume a specific weighting of capability, intent, and targeting. However, it does assume that an organization will use the same weighting across all the adversaries it considers relevant to a mission or business function, or to the organization as a whole.

Consider the Temporal Aspect of the Threat

Intent, capability and targeting – and the possible consequences of a detected attack to the adversary – change over time. In general, organizations do not have current and well-founded threat intelligence; at best, they only know what they (or their peers or partners) have seen in the past or present. Even when it detects evidence of an intrusion, an organization can face difficulties determining whether the detected attack is part of a longer-term pattern of activity.

Organizations differ in how they consider well-informed predictions or speculations regarding changes in adversary intent, capability, and targeting.[3] Some organizations are forward-leaning, particularly with respect to capability, assuming that an adversary that has a higher level of intent and targeting than of capability will in time acquire commensurate capability. Other organizations treat the past as predictive.

Organizations also differ in their interpretations of detected activity. Some interpret events narrowly, assuming that the observed consequences (e.g., exfiltration, privilege escalation) – together with some proximate possible additional consequences (e.g., continued disclosure of sensitive data, access to additional sensitive data) – constitute the adversary's goal. Such organizations thus infer that the tradecraft or TTPs in evidence accurately represent the adversary's capabilities. Other organizations assume an advanced *persistent* threat. Such organizations analyze observed consequences as preparatory for future attacks; they assume that the adversary wants to hold some tradecraft in reserve for the future, and thus infer a more comprehensive set of capabilities than evidenced by observed TTPs.

While Cyber Prep accommodates a wide range of attitudes toward predictions, the higher levels of preparedness assume the advanced persistent threat and encourage a forward-leaning stance.

Consider Adversaries Specific to Different Business Functions or Missions

Federated organizations are characterized by shared resources but multiple business functions or missions. That is, in a federation, each organization has its own business function mission; these collectively contribute to the mission of the federation. Different functions or missions may have different adversaries and hence need to prepare for different TTPs.

[3] The public body of knowledge about the advanced persistent threat is growing, as is the body of speculations and predictions. The latter varies in quality from well-informed to hyperbolic. Each organization needs to determine which sources it takes seriously as an input into strategic planning and risk analysis.

The recommended approach is to assume the worst case (maximum adversary level) to determine the federated organization's overall Cyber Prep level. This worst-case assumption informs cyber security governance, planning, and risk management for shared resources. The organization needs to identify shared resources and use all worst-case TTPs to determine which safeguards to apply to those resources. In the evolution of the enterprise architecture, the organization should plan to adopt some of Cyber Prep Level 4 security measures (e.g., network segregation) to ensure adequate isolation of components. Individual component organizations can make their own assessments of the adversaries they face. Component organizations can then use the TTPs specific to their adversaries to determine which safeguards to apply to their resources.

Conclusion

Cyber Prep enables an organization to base its cyber security strategy on an assessment of the level of cyber threat it faces. This allows an organization to identify relevant TTPs and select security controls or safeguards based on its adversary's capability, intent, and targeting. For convenience, Cyber Prep provides five levels of adversary characterization. However, when the levels of its adversary's capability, intent, and targeting vary, an organization needs to decide what overall threat level to prepare for. The way an organization combines separate assessments of capability, intent, and targeting to produce an overall assessment of threat level reflects its attitude toward adversary behavior, risk, and uncertainty. Cyber Prep accommodates different attitudes. By providing a set of anchoring examples, this white paper can help an organization determine which method of combining separate assessments into overall threat level best suits it.

References

[1] Bodeau, D., Graubart, R., and Fabius-Greene, J., *Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels*, The MITRE Corporation, 2009, PR 09-4656, http://www.mitre.org/work/tech_papers/2010/09_4656/09_4656.pdf

[2] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009, http://www.ndia.org/Advocacy/PolicyPublicationsResources/Documents/Cyberspace_policy_review_2009.pdf

[3] Department of Defense, National Military Strategy for Cyberspace Operations, 2006, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

[4] International Telecommunications Union (ITU) Study Group 17, Overview of Cybersecurity, Draft ITU-T Rec. X.1205, 2008

[5] U.S. Department of Homeland Security (DHS) Risk Lexicon, September 2008, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

[6] The Open Group, Technical Standard: Risk Taxonomy, 2009, available from http://www.opengroup.org/pubs/catalog/c081.htm

[7] National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology Systems, NIST Special Publication (SP) 800-30, 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[8] Shelby Evans, David Heinbuch, Elizabeth Kyule, John Piorkowski, James Wallner, "Risk-based Systems Security Engineering: Stopping Attacks with Intention," *IEEE Security and Privacy*, vol. 2, no. 6, pp. 59-62, Nov. 2004, doi:10.1109/MSP.2004.109

[9] Bud Whiteman, "Network Risk Assessment Tool," IA Newsletter, Vol. 11 No. 1, Spring 2008, http://iac.dtic.mil/iatac/download/Vol11_No1.pdf

[10] David P. Duggan, Sherry R. Thomas, Cynthia K. K. Veitch, and Laura Woodard, Categorizing Threat: Building and Using a Generic Threat Matrix, Sandia Report SAND2007-5791, September 2007, http://www.oe.energy.gov/DocumentsandMedia/Categorizing_Threat.pdf

[11] David P. Duggan and John T. Michalski, Threat Analysis Framework, Sandia Report SAND2007-5792, September 2007, http://www.oe.energy.gov/DocumentsandMedia/Threat_Analysis_Framework.pdf

[12] Richard J. Harknett, John P. Callaghan, and Rudi Kauffman, Rudi, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management*: Vol. 7, Issue 1, Article 22, 2010, available at http://www.bepress.com/jhsem/vol7/iss1/22

[13] Verizon Business RISK Team, 2009 Data Breach Investigations Report, 2009, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, and 2009 Data Breach Investigations Supplemental Report: Anatomy of a Data Breach, 2009, http://www.verizonbusiness.com/resources/security/reports/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf

[14] Wayne Henry, Jacob Stange and Eric Trias, "Pearl Harbor 2.0: When Cyber-Acts Lead to the Battlefield," The Proceedings of the 5th International Conference on Information Warfare and Security, The Air Force Institute of Technology, Wright-Patterson AFB, Ohio, USA, 8-9 April 2010, pp. 148-154

[15] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in Networks and Netwars: The Future of Terror, Crime, and Militancy, edited by John Arquilla and David Ronfeldt, 2001, RAND Monographs/Reports, MR-1382-OSD, http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

[16] Office of the National Counterintelligence Executive (ONCIX), Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008, NCIX-007-09, 23 July 2009, http://www.ncix.gov/publications/reports/fecie_all/fecie_2008/2008_FECIE_Blue.pdf

[17] Cisco, Cisco 2009 Annual Security Report, 2009, http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf

[18] MANDIANT, M-Trends Report, January 2010, available from http://www.mandiant.com/products/services/m-trends

[19] Center for Strategic and International Studies (CSIS), Significant Cyber Incidents Since 2006, 10 April 2010, http://csis.org/files/publication/100420_CyberEventsSince2006.pdf

[20] *The Economist*, "Cyberwar: War in the fifth domain," 1 July 2010, http://www.economist.com/node/16478792

Appendix A: Examples of Adversary Scenarios and Alternative Assessments of Adversary Level

Table 3 presents a set of anchoring examples or scenarios, using the following representative types of adversaries, with non-uniform levels of capability, intent, and targeting:[4][5]

1. Zealots
    a. Hacktivist / Ad-hoc group
    b. Well established group such as a terrorist organization
    c. Deranged individual
2. Insiders
    a. Lone individual
    b. Individual with connections to or relationships with external adversaries
3. Organized Crime
    a. Group which primarily engages in criminal activity in the physical world with limited cyber presence
    b. Group which primarily engages in criminal activity online
4. Nation-state
    a. Nation-state with moderate ability to act within a geographic area , which places greater reliance on physical proximity and traditional intelligence tradecraft
    b. Nation-state with sophisticated capabilities to act with a near-global reach
    c. Sophisticated nation-state allied with U.S.
    d. Sophisticated nation-state often, but not always, working with U.S.

An organization could use any of a variety of ways to combine different levels of capability, intent, and targeting into an overall threat level. An organization's choice of how to combine these factors reflects its attitude toward risk, including its overall tolerance for uncertainty (i.e., the degree of uncertainty the organization is willing and/or able to tolerate in making decisions that involve possible loss), its specific tolerances toward uncertainty in different risk factors (in this case, the three factors used to characterize an adversary), and its weighting of risk factors.

In Table 3, several representative risk attitudes – reflecting different ways of combining capability, intent, and targeting – are suggested:

a. A risk-averse organization could see threat as the maximum of the three factors.
b. A risk-tolerant organization could see threat as the minimum of the three factors.
c. An organization could focus solely on the adversary's capability.
d. An organization could focus solely on the adversary's intent.
e. An organization could assume that if the adversary's intent is greater than its capability or targeting, that intent will lead the adversary to increase either its capability or its targeting. Such an organization might compute the adversary's level by computing the maximum of capability and targeting, and then taking the minimum of that value and intent.

[4] The Cyber Prep methodology does not establish a taxonomy of adversary types. Taxonomies are being proposed (see, for example, [13, 14]), but Cyber Prep assumes that an organization will use the taxonomy best suited to it. This listing is for purposes of illustration and elucidation only, and is not intended to be complete.
[5] These examples are derived from a variety of sources, including [13-20].

Table 3 illustrates how these different risk attitudes result in different assessments of adversary level for the representative scenarios. Cyber Prep intentionally does not assume a specific attitude toward risk. Specific equities, sensitivities and/or perspectives shape how organizations weight the input factors to determine the overall threat. Because defense resources are allocated across organizations differently, Cyber Prep was designed to be flexible enough to allow multiple approaches without requiring an organization to retrofit its processes into Cyber Prep.

Table 3. Examples of Alternative Ways to Assess Adversary Level

Adversary	Scenario Description	Assessments of Adversary Characteristics	Alternative Assessments of Adversary Level
1.a	A hacktivist wants to embarrass a type of or a specific organization, agency, or company for its actual or perceived support for US military operations overseas by placing demoralizing content on its website.	Capability: 1 Intent:1 Targeting:3	a. 3 b. 1 c. 1 d. 1 e. 1
1.b	An extremist group uses the Internet to conduct initial reconnaissance on prospective targets and identifies some candidates that would allow it to not only bring physical harm but have more extended ripple effects by damaging the critical infrastructure it manages. Based on their knowledge of the candidate targets, they decide to pursue one particular one because of its reputation for having cyber security problems (which will allow them to use existing exploits rather than use their limited supply of new ones) along with their ability to penetrate its physical perimeter with relative ease.	Capability: 3 Intent:5 Targeting:4	a. 5 b. 3 c. 3 d. 5 e. 4
1.c	A deranged individual has a misplaced belief that a particular US Government (USG) agency is collecting slanderous information on him/her and therefore has fixated on harming the cyber operations of the organization. The individual, while intelligent, lacks any training in cyber operations, does not have any more access to the organization's cyber operations than any other citizen, and does not personally know any employees of the agency.	Capability: 1 Intent:5 Targeting:3	a. 5 b. 1 c. 1 d. 5 e. 3
2.a	A disgruntled system administrator wants to punish his organization for not hiring his girlfriend despite his two years of loyal service. So he uses his position to covertly obtain sensitive, embarrassing information regarding organization operations that he secretly leaks, over a period of time, to the media.	Capability: 4 Intent:3 Targeting:3	a. 4 b. 3 c. 4 d. 3 e. 3

Adversary	Scenario Description	Assessments of Adversary Characteristics	Alternative Assessments of Adversary Level
2.b	An animal rights activist group with tech savvy members wishes to "punish" USG agencies involved in R&D that utilizes animals for testing. Their modus operandi is to use their extensive network of members to find those who have friends or family that work for such USG agencies. The group then uses social engineering techniques (e.g., malicious birthday card email from the group member that has relationship with the USG employee) to get the unsuspecting employee to install a malicious rootkit on the agency's systems. If the technique is successful, the group then continues and extends the unsuspecting user access to establish a more extensive presence and extricate information that the group can subsequently use to target specific programs and individuals.	Capability: 3 Intent:4 Targeting:3	a. 4 b. 3 c. 3 d. 4 e. 3
3.a	A sophisticated criminal organization desires to gain access to large quantities of personally identifiable information (PII) maintained by financial organizations. While the criminal organization lacks any cyber presence, it has long experience in identifying individuals with appropriate skills and access and then co-opting individuals to take actions that help the criminal organization achieve its goals. It is able to use this experience to find suitable individuals (e.g., employees who are either disgruntled or subject to blackmail and with privileged user access) who have access to personal information on thousands of people who provided information to that agency. That information can be used subsequently to obtain bank and credit card information so that the criminal organization profits significantly from the theft of the information.	Capability: 3 Intent:3 Targeting:4	a. 4 b. 3 c. 3 d. 3 e. 3
3.b	An established Eastern European hacker group in pursuit of quick money focuses on an extortion scheme against select Fortune 500 companies and specifically pursues the IT managers with threats. Using their capabilities to establish extended botnets, they demand money within a certain timeframe or threaten to cripple their IT capabilities.	Capability: 4 Intent:4 Targeting:4	a. 4 b. 4 c. 4 d. 4 e. 4
4.a	A nation state that periodically has heated international disputes with the US wants to set the stage so that when future conflicts occur they have the capability to modify or delete select portions of USG agencies' data at their time and choosing. To carry this off, they have identified the primary contractors in the Defense Industrial Base likely to be supporting the military in their country and have obtained access to multiple facilities and been able to take advantage of well-intentioned, helpful employees that were willing to download a file for them when their computer was not cooperating.	Capability: 3 Intent: 4 Targeting: 5	a. 5 b. 3 c. 3 d. 4 e. 4

Adversary	Scenario Description	Assessments of Adversary Characteristics	Alternative Assessments of Adversary Level
4.b	An aggressive and hostile nation state with major capabilities in the cyber arena has identified the Department of XYZ's preferred IT providers and has managed to make a subsidiary under its control the primary supplier of computer chips for those systems. It has some covert connections to Department XYZ's primary IT O&M support. It has also co-opted two 8A firms that have an increasing presence in the manufacturing of select software for an agency within Department XYZ. Through the computer chip provider, they have been able to install a program that has not been previously detected publically that be called upon remotely to be activated.	Capability: 5 Intent:4 Targeting:5	a. 5 b. 4 c. 5 d. 4 e. 4
4.c	A nation which is a long-time ally of the U.S. works to build up its already considerable cyber capabilities. The nation and the U.S. share geo-political philosophies and have a history of sharing information including intelligence. Organizations and nations that this nation perceives as hostile almost always are similarly perceived by the U.S.	Capability: 5 Intent:1 Targeting:1	a. 5 b. 1 c. 5 d. 1 e. 1
4.d	A nation has considerable cyber capabilities. The nation has been known to work cooperatively with the US against common foes, and the U.S. is a major supporter of the nation. However, the nation places a paramount importance on ensuring it has the most up to date information on its adversaries. As such, the nation may target USG personnel who are sympathetic to the nation's needs and have access to information that would aid the nation in regards to its adversaries.	Capability: 5 Intent:3 Targeting:4	a. 5 b. 3 c. 5 d. 3 e. 3