SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact

By Charles Harry, PhD

CISSM Working Paper

July 2015

This paper was made possible with the generous support of the Yamamoto-Scheffelin Endowment for Policy Research.

Center for International and Security Studies at Maryland
4113 Van Munching Hall, School of Public Policy
University of Maryland
College Park, MD 20742
(301) 405-7601

Abstract

While significant media attention has been given to the volume and range of cyber attacks, the inability to measure and categorize disruptive events has complicated efforts of policy makers to push comprehensive responses that address the range of cyber activity. While organizations and public officials have spent significant time and resources attempting to grapple with the complex nature of these threats, a systematic and comprehensive approach to categorize and measure *disruptive* attacks remains elusive. This paper addresses this issue by differentiating between exploitive and disruptive cyber events, proposes a formal method to categorize five types of disruptive events, and measures their impact along three dimensions of analysis. Scope, magnitude, and duration of disruptive cyber events are analyzed to locate each event on a Cyber Disruption Index (CDI) so organizations and policymakers can estimate the aggregated effect of a malicious act aimed at impacting their operations. Using the five different event classes and the CDI estimation method makes it easier for organizations and policy makers to disaggregate a complex topic, contextualize and process individual threats to their network, target where increased investment can reduce the risk of specific disruptive cyber events, and distinguish between events that represent a private-sector problem from those that merit a more serious public-sector concern.

Introduction

The reliance of modern life on the large number of interconnected networks of computers, infrastructure, and sensors has made the threat of disruption a growing concern among business leaders and policy makers. Network security is increasingly seen as a strategic vulnerability as a growing number of corporate intrusions are reported. In fact, in 2014 over 1,541 breaches to company networks were identified.[1] These breaches affect customer privacy, confidence in a company's ability to protect core intellectual property, and an organization's essential operations.[2] Large numbers of intrusions have also occurred into government networks, with recent high-profile breaches including a significant compromise at the Office of Personal Management.[3]

As both the private and public sectors grapple with the problem of cyber "attack," disagreement remains regarding what can and should be done about the problem. This confusion reflects lack of clarity regarding the threat itself, which in part originates from the lack of precision in how we categorize and measure the range of disruptive cyber events. For example, a hacker takeover of a government social media account would not be nearly as disruptive as deleting the files on more than 30,000 computers in the internal network of that same organization. Individuals, organizations, and policy makers cannot decide how serious the problem is, what they should be most concerned about, and how much they should be willing to pay (in money, decreased privacy, efficiency, and flexibility) to prevent, defend against, or recover from a "cyber attack."

While some measures exist to quantify the *vulnerability* posed from malware and computer exploits, there is currently no approach to quantify the relative differences between or to estimate the total effect of *disruptive events*.[4] To address this gap, I first differentiate between computer exploitation and cyber disruption, then formalize a Cyber Disruption Index (CDI) that allows for a repeatable and logically consistent approach to estimating the magnitude of any disruptive cyber event based on its scope, magnitude, and duration. Leveraging the CDI, I establish taxonomy of five groups of cyber disruption defined by the tactics employed by a malicious actor. Organizations can use this framework to categorize and estimate the effects of a range of potential disruptive cyber threats, clarifying between attacks that can cripple critical operations from those that are merely a nuisance. Policy makers can also apply the approach in this paper to differentiate between cyber attacks that pose more serious concerns to the broader society thereby allowing for a deeper understanding of the threat posed and a means to identify the organizations and industries that may require additional oversight.

Generic terms, understandable confusion

Recent disruptive cyber events, including those at the Sony Corporation and Saudi Aramco, have spawned discussion about how to characterize threats, and which defensive measures that should

[1] http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf
[2] Ibid
[3] Davidson, J " http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/new-opm-data-breach-numbers-leave-federal-employees-anguished-outraged/"
[4] The Common Vulnerability Scoring System (CVSS) is the most widely used. For more information see: https://nvd.nist.gov/cvss.cfm

be taken.[5] Policy makers, including President Obama, have spent considerable effort strengthening the U.S. ability to prevent or respond to such attacks.[6] These events raise two important questions. First, which entities constitute part of critical infrastructure or are of such importance to the economy that the disruption of activity at that location would present significant social consequences? The second, which type of attacks or techniques should the people who run these entities be most concerned about and what should they be doing to reduce risk both to the organization itself and to the society that depends on it? Policy makers have expended significant attention on answering the first question, identifying though executive action and implementing through statute, requirements to address vulnerabilities in critical infrastructure.[7] The second question is equally important but has received much less attention.

While the government has worked to address cyber threats with dozens of initiatives in the past several years, the proposed solutions treat the threat as monolithic, ignoring the real differences in motivation, tactics, and impact to the targeted networks.[8] Social media account compromises are lumped together with large-scale data breaches, which are muddled with potential core infrastructure disruptions. In fact the overuse of terms such as "cyber attack," "cyber war," "cyber terrorism," or "cyber intrusion" creates a single category of event that fails to differentiate among the wide range of potential disruption scenarios. Typical of this problem is Valeriano and Maness' 2012 article in *Foreign Affairs*, which uses both STUXNET and the FLAME tool as examples in their discussion concerning "cyberwarfare." In fact, STUXNET is a tool leveraged to disrupt Iranian enrichment activity, whereas the FLAME toolset appears to be focused primarily on cyber espionage.[9] Lumping these types of events together into a single category complicates both our understanding of any individual scenario and makes it impossible to compare and contrast differing espionage or disruptive events.

This one size fits all definition does not allow businesses or governments to concentrate on defending and hardening the most important elements of their communications networks. The language describing a wide range of activities—from compromise of information to wholesale destruction of infrastructure equipment—is mixed up into a couple of terms that are often loosely thrown around. For example the term computer network exploitation is typically a variant of the following definition:

> "Computer network exploitation (CNE) is a technique through which computer networks are used to infiltrate target computers' networks to extract and gather intelligence data. It enables the exploitation of the individual computers and computer networks of an

[5] Gallagher, S "Inside the wiper malware that brought Sony Pictures to its knees" http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/; Symantec ,"The Shamoon Attacks" , Symantec Blog, August 2012 http://www.symantec.com/connect/blogs/shamoon-attacks

[6] http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

[7] Executive Order 13636—Improving Critical Infrastructure Cybersecurity; CSIS. "Cyber Legislation," CSIS Technology and Public Policy Blog, June 17, 2011.

[8] Ibid.

[9] Valeriano and Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live up to the Hype", https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar, Foreign Affairs, August 2012; http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

> external organization or country in order to collect any sensitive or confidential data, which is typically kept hidden and protected from the general public."[10]

This definition appears sensible and in line with the clandestine accruing of computing resources for purpose of financial or intelligence gain. However, popular media, organizations, and government officials have also used the term cyberwar or the more generic cyber attack to describe similar events. Reviewing a common definition:

> "A cyber attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft."[11]

The use of generic and duplicative terms when describing cyber activities has led to confusion over what constitutes a true threat to an organization's operations and the inability to distinguish between often radically differing cyber events. Both computer exploitation and computer network attacks are important topics, but the inability to distinguish event types has made the task of specifying the scope and magnitude of disruptive events nearly impossible. ***This paper defines events that seek to impact an organization's ability to produce and deliver a good/service, or to communicate with its target audience as a disruptive cyber event.*** This definition is distinct from cyber/computer exploitation that can be defined as a technique through which computer networks are used to infiltrate target computers' networks to extract and gather intelligence data.[12] While certain disruptive cyber events would likely follow on from a computer that has been exploited, a disruptive event is different in that the attacker intends to cause disruption to the operations of an organization versus a compromise of data for purposes of criminal gain, intelligence gain, or intellectual property theft.

Disruptive attacks are the focus of this paper as they are the operations that pose the most direct threat to the supporting infrastructure of modern society. I propose that specific types of disruptive attacks are more concerning than others and that those events that are most likely to significantly disrupt should be the focus of greater private investment and government oversight. While computer exploitation leading to the compromise of personal data or intellectual property is a significant concern, I do not address it in this paper.

Defining cyber disruption and the dimensions for analysis

While all disruptive cyber events aim to affect an organization's ability to produce, deliver, or communicate with its target audience, a malicious actor may utilize multiple tactics that have wildly different disruptive outcomes. These events might include the deletion of data across a wide range of corporate networks, the destruction of physical equipment used to produce goods, an attempt to prevent users from reaching a website, or the denial of access to a social media account. Given the wide range of disruptive events it is useful to categorize events by using both

[10] http://www.techopedia.com/definition/27909/computer-network-exploitation-cne
[11] http://www.techopedia.com/definition/24748/cyberattack
[12] http://www.techopedia.com/definition/27909/computer-network-exploitation-cne

the tactics employed by the attacker and by measuring the impact of the event itself. To measure the impact of the disruptive event we might consider: where the event occurs in a network topology, the magnitude of the effect, and the length of time the disruption affects the organization's operations. There are three framing questions that must be answered for any given disruptive event. These include:

- What is the scope of the disruption?
- What is the magnitude of the disruption?
- What is the duration of the disruption?

The scope of a disruptive event is a function of a computer network's topology, the number of computers or equipment affected, and the importance of those computers to the overall network. While shear numbers of impacted computer systems are one factor contributing to the scope of the action, the importance of a specific system in that network may matter more than thousands of other devices. For example, corporations that use virtualization technologies to quickly scale and efficiently maintain their networks may find that their inability to use the high-end servers that provide virtual machine images to their employees has broader implications than taking 100 client machines offline.

The magnitude of a disruptive event is tied to the impact a malicious actor has on the key underlying services that support an organization's key production functions. If an organization's production of goods or services is tied to the deployment of labor, capital, and technology, then interruption of technology that enables the interaction of labor and capital is the key determinant of the magnitude of the event. The range of disruptive magnitude therefore is directly tied to the productive capacity of the underlying computer systems. For example, a computer used by employees to send emails and other correspondence may not be as productive as the device that controls automated assembly in a manufacturing plant. So while both devices have some productive value to the enterprise, the ability to differentiate the magnitude of impact is a key factor in our analysis.

The duration of an event is the third dimension of our analysis. Along with the scope and magnitude of a disruptive event, understanding the duration of an event along with the spillover effects it may have on an organization's operations is critical to differentiating between event types. The use of a botnet to launch a DDOS-type attack against a firm's webserver is likely to last from minutes to perhaps a day. That event differs significantly from a situation in which a malicious actor is able to modify a control system in a manufacturing plant, potentially destroying physical capital and causing production slowdowns for months.

It is possible in theory to specify a mathematical model that synthesizes these three dimensions into a single measure of cyber disruption.[13] If we assume a network exists of j+n nodes we can combine our three dimensions of analysis for all time periods (t+m) into the following equation for a Cyber Disruption Index (CDI):

[13] A detailed treatment of the derivation of the CDI can be found in the appendix to this paper.

$$CDI = \sum_{t}^{m} \sum_{j}^{n} C_j \left(\frac{DET_{j,t}}{PCT_{j,t}} \right)$$

$Where$:

$C_j = Centrality\ score\ for\ node\ J\ (assumed\ constant\ over\ t)$
$DET = Disruptive\ Effect\ of\ Technology\ (DET \leq PCT)$
$PCT = Productive\ Capacity\ of\ Technology$

j= Nodes in Graph G
t=Time Periods

We define the scope of the event by summing across all the nodes in a network and multiplying by importance (centrality). The magnitude of the event is the defined as, for each node, the ratio of the disruptive effect on a node to its productive capacity. This enables us to estimate the portion of production for each node that is "disabled" due to a disruptive cyber event. Finally, the product of the scope and magnitude is summed over time to account for the duration of the disruptive event. The score, or CDI, represents a single value that accounts for the three dimensions of analysis. That value can be used as a means of ranking events, thereby establishing a means of comparative analysis.

While a mathematical approximation is useful conceptually, a number of practical difficulties, such as gaining access to highly detailed information concerning which network components are affected, make use of the formulation challenging. However, the structure it provides can allow us to approximate the scope, magnitude, and duration of an event. Figure 1 lays out a simple chart with the event's scope on the x-axis, magnitude on the y-axis and duration represented by the size of the event marker. This allows us to use qualitative assessment (e.g. low, medium, high), rather than precise measurement (e.g. 10,300 computers), to broadly define the overall disruptive character of an attacker's actions.

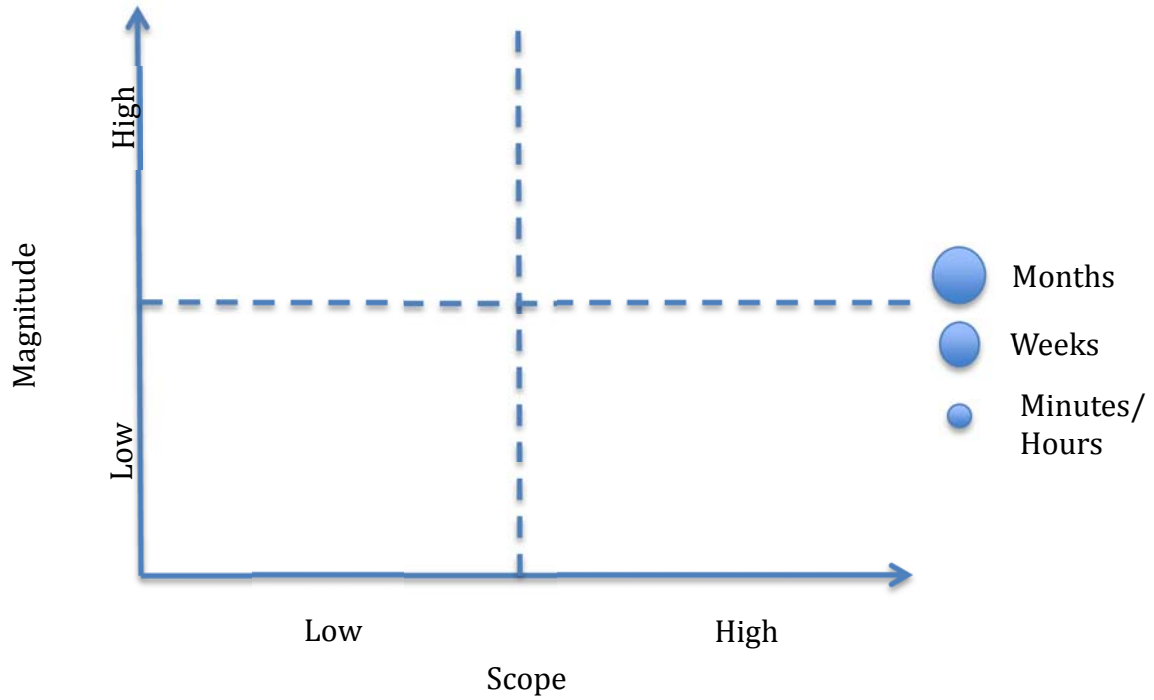


Figure 1: Dimensions of the Cyber Disruption Index

Utilizing this visual method for estimating the magnitude of an event, we can take news accounts and technical reviews of cyber disruptive events and approximate the impact they have had on the targeted organization. In the following sections, I make use of this estimation method to analyze five disruptive cyber events that each involved differing tactics employed by a malicious actor to achieve a desired impact.

Classifying Disruptive Cyber Events

I propose that five distinct classes of disruptive cyber events exist based on the tactics used by a malicious actor to disrupt a targeted network. Each class embodies distinct differences from one another through the combination of: the scope of the network topology impacted, magnitude of the event in the network, and the duration of the disruption to the network. The five classes are defined as:

1) Message Manipulation: Disruption of an organization's social media presence through the hijacking of a user's account passwords;
2) External Service Disruption: Disruption of external operations through a distributed denial of service attack (DDOS);
3) Internal Communication Disruption: Disruption of internal operations through a denial of service;
4) Data Attack: Disruption of internal operations through internal multi-point deletion or encryption of user data; and
5) Equipment Attack: Disruption of internal operations by physically destroying or disabling equipment control capabilities; and/or access to electric power or other critical infrastructure.

Our use of this classification enables us to compare events in the same class or to compare events in separate classes. Each disruptive event type identified above is emblematic of differing strategies and tactics employed by attackers of a target network. In the figure below, a sample corporate network is laid out, including web servers, routers, a data center, corporate departments and their computers, and finally production systems connected to the network (represented by gears).

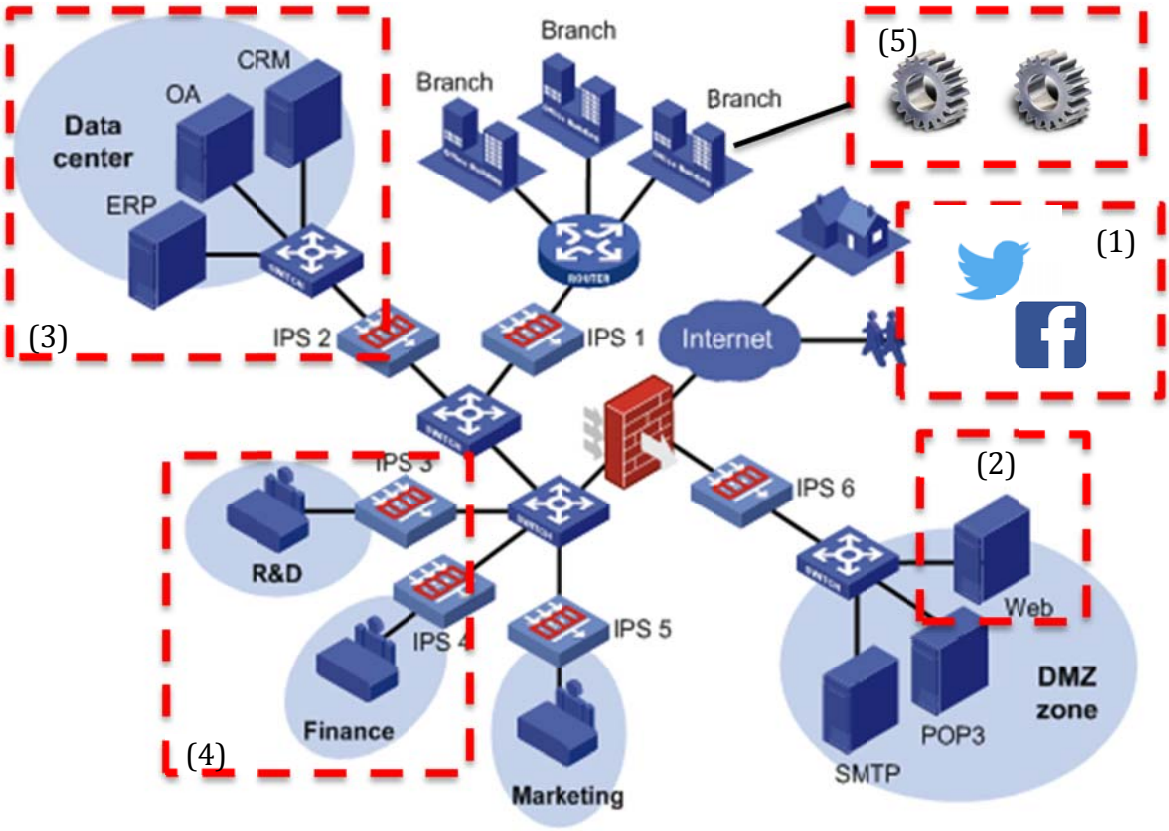


Figure 2: Types of Cyber Disruption Events

Message Manipulation events involve the organization's accounts hosted by external applications such as Facebook or Twitter. External service disruption events target externally facing systems such as a web server that would host the website of an organization. Internal communications disruption events typically affect a few systemically important appliances such as a router or data center. With data attack events, end-user computers, typically across large sections of the corporation, are targeted. Finally, equipment attack events impact the control systems that interact with production equipment.

Each class of event, while belonging to the general category of cyber disruption, requires differing levels of skill, access, and planning to have the intended effect. Compromising account passwords can be as simple as guessing user credentials, while accessing and destroying physical infrastructure takes significant resources, knowledge, and time.[14] Breaking down event classes therefore is an important process to help understand and remediate vulnerabilities to important communications systems.

Message manipulation: Disruption through hijacking of a user's personal social media accounts

Many events that are deemed "cyber attacks" are often the result of a simple compromise of a personal social media account. While not overly sophisticated, the ability for an attacker to hijack public communications of a target does have some disruptive effect as was seen in the January 2015 compromise of a U.S Central Command (USCENTCOM) social media account by the Islamic State of Iraq and Levant (ISIL). [15]

In this case, self-identified ISIL cyber operatives gained access to the Twitter and YouTube accounts used by USCENTCOM and posted messages threatening service members. The attackers were never inside U.S. military systems, but the large amount of publicity surrounding the event achieved the apparent goal of the group to leverage a cyber event to disrupt USCENTCOM's normal external communications channel. The ISIL compromise was temporary as the site was returned to normal use within 30 minutes.[16]

The characteristics of a Message Manipulation event include:

- attacker has access to an account used for communication, but access is external to a victim's corporate network;
- no damage of critical or end-host systems; and
- victim can easily remediate by having service provider reset password.

The scope of an account hijack tends to be small or insignificant with user accounts being targeted and not their computers. Further, as social media accounts tend to be a service outside of a victim's home network, these disruptive events are not an important node in the victim's network; they are hosted by third-party providers (e.g., Facebook). These events therefore tend to be characterized as having a small scope relative to other types of disruptive events.

The magnitude of this type of disruptive event is often small in size, as social media accounts or webpages can easily be recovered. The underlying data that is used to provide updates on social

[14] Falliere, Murchu,and Chien " W32.Stuxnet. Dossier" http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011.
[15] Lamothe, D "U.S military social media accounts apparently hacked by Islamic State sympathizers" , http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/, Washington Post, January 2015.
[16] Ibid

media accounts is not touched, thereby allowing victims of this type of event to easily recover from the hack, as the productive capacity to produce a good is never effected. While an organization's communications with a target audience is impacted, the core capability to deliver a good or service to market is not seriously affected, and therefore the magnitude of the event is often assessed to be low.

The duration of a disruptive event involving hijacked social media credentials is directly related to the speed by which a hosting service (e.g., Twitter or YouTube) can reset a user account. Given that these types of events do not impact the underlying computer network, access to the account is easily returned to the legitimate user by simply resetting the credentials (password). The duration of these types of events are therefore often resolved in a very short timeframe (e.g., minutes or hours).

Applying our analytic process to the example of the ISIL compromise of the CENTCOM social media presence, we find that this event had: a low scope with the only affected system being the social media accounts of CENTCOM; a low level of magnitude, as no internal systems were damaged; and finally a short duration, with the account being reset in under an hour. Visually we can plot this event noting that its overall disruptive effect to the intended target (CENTCOM) is minor.

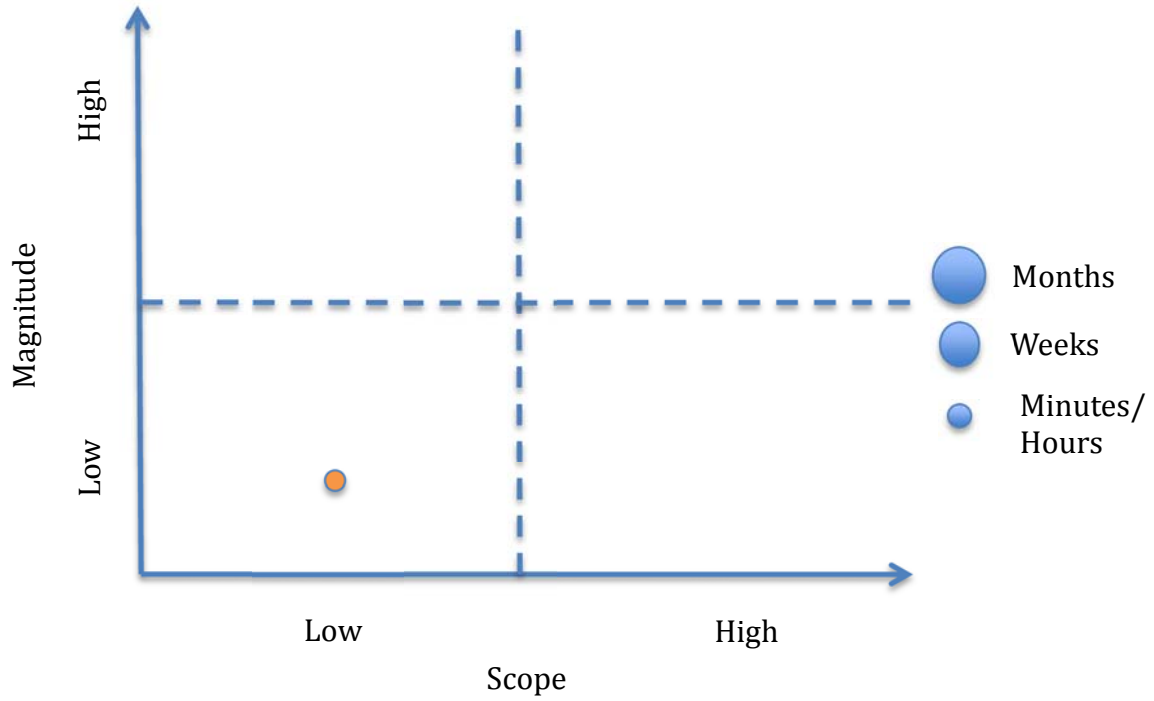


Figure 3: CDI Estimate for ISIL's Compromise of the CENTCOM Social Media Presence

External service disruption: Disruption of external operations through a DDOS attack or website defacement

While account hijacking is common, it is not often associated with computer disruption. A more recognizable type of disruptive event is the external flood of requests to a website server, with the aim of overwhelming its ability to meet the demand. The result is an inability to address legitimate requests, leading to an error for the user. This disruptive event known as a distributed-denial-of-service (DDoS) attack occurs thousands of times per day, across a range of organizations around the world.[17]

On April 27, 2007, a local dispute surrounding the movement of a Russian war memorial manifested itself into a series of DDoS events on 9 different Estonian government networks. Seventy-five percent of the 128 DDoS events that day were resolved in an hour, yet the publicity surrounding the events brought accusations that the Russian government was behind the attacks.[18] No critical government operations were impacted by the DDoS event, and it was later found that a private citizen with Russian sympathies was behind the event and not the Russian government.

While the techniques associated with the execution of a DDoS event can change, its core characteristics include an attacker, external to an organization's network, who floods a webserver or externally facing server with requests that overwhelm and prevent legitimate traffic from being responded to. Many DDoS attacks are small in scale and easily defeated, but increasingly large attacks have become more common with more than 25 attacks of 100 gigabites per second (Gbps) being recorded in the first quarter of 2015.[19] The characteristics of external service disruption events include:

- attackers use externally controlled systems to overwhelm a victims' outward facing systems (e.g., no access to internal systems);
- attackers attempt to deny external users access to the victim network (e.g., customers vice employees); and
- attacks are often limited in duration, as system administrators and upstream Internet Service Providers are able to filter out attacks.

The figure below highlights the structure of a DDoS attack: the command and control server, the network of compromised computers that generates the requests, and the victim web server.[20]

[17] According to Arbor Networks, the global internet sees over 2,934 DDOS attacks per day. http://www.arbornetworks.com/resources/research/attack-map.
[18] Traynor, I "Russia accused of unleashing cyberwar to disable Estonia ,http://www.theguardian.com/world/2007/may/17/topstories3.russia, Guardian, May 2007.
[19]Dunn, J "Asian Datacentre hit by massive 334 Gbps DDoS Attack, Arbor Networks reveals", http://www.techworld.com/news/security/asian-datacentre-hit-by-massive-334gbps-ddos-attack-arbor-networks-reveals-3609764/, Techworld, April 2015.
[20] Figure borrowed from the NSFOCUS Blog http://nsfocusblog.com/2012/10/29/ddos-attack-and-defense/

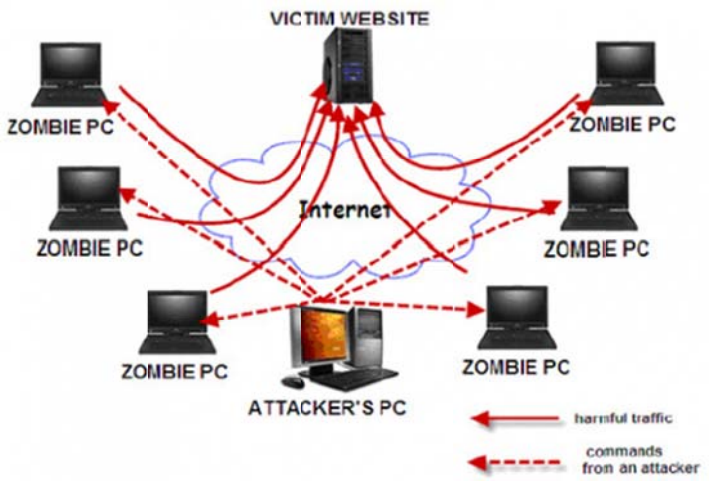


Figure 4: Sample Configuration of a DDoS Attack[21]

The scope of an external DDoS is typically a single node that is externally facing, and the attacker is outside of the organization's network. These single-node targets tend to be the computer infrastructure of organization's external web presence. The attacker generates a series of requests from his botnet and hopes to overwhelm the ability of the target to handle the traffic.[22] If successful, the attacker prevents other legitimate users from being able to visit the website. In our example of the Estonian DDoS, some webservers were unresponsive for hours, with external users unable to access information resident on the website for several government ministries. No internal systems were compromised or damaged in the event; individual, externally facing systems were the only victims.

The magnitude of DDoS events can vary and is largely dependent upon the value the organization places on its external web presence (e.g., importance of the website to their operations). For example, a large steel manufacturer who loses the ability to display their webpage for 17 hours is likely not to incur a large disruptive effect, whereas a large retailer who relies heavily on online purchases may find this type of event extremely disruptive to their business. In some cases, large and directed DDoS events can overwhelm an organization's ability to deal with the traffic. Large attacks (greater than 100 Gbps) aimed at a smaller organization or at a datacenter that serves multiple businesses can have a significant impact on the ability to maintain operations. In the case of the 2015 DDoS event affecting the Great Fire organization, a sustained DDoS event leveraged unwitting internet users to open up hundreds of thousands of connections that kept the organization's website offline for weeks.[23] As the organization's mission was to promote ways to bypass Chinese censorship, its ability to meet these objectives was blocked for a considerable period of time. In our earlier example of the Estonian DDoS event, the productive capacity of the government website was limited. While largely a nuisance, no central government services were disrupted.

[21] Image from http://trapple.nl/content/denial-service-attacks-ddos-and-dos-cyber-attacks-explained
[22] A Botnet is a group of computers that are controlled by a individual who wants to coordinate a group action such as a DDoS.
[23] Citizenlab "China's Great Cannon", https://citizenlab.org/2015/04/chinas-great-cannon/, Citizenlab Blog, April 2015.

The duration of external DDoS disruptive events can vary from minutes to weeks depending on the sophistication of the attacker. The vast majority of DDoS events are remedied through filtering of IP addresses that are implicated in the attack, thereby quickly reducing the ability of the attacker to severely disrupt the operations of an organization's webserver. While on average most attacks last only 17 hours and are primarily aimed at disrupting outward facing network devices, the growing number of large bandwidth attacks against large datacenters signals a troubling trend.[24]

Applying the three dimensions of analysis to the example of the Estonian DDoS, we find that this event had a slightly higher scope than the ISIL operation targeting CENTCOM social media accounts, with the Estonian government's web servers directly targeted. However, the magnitude of the event is still low, as no internal systems were damaged. The duration of the event, while longer than the CENTCOM account compromise, was mostly resolved in one day. We can plot this event noting that its overall disruptive effect to the intended target is low in scope and magnitude and was resolved in hours (<24 hours).

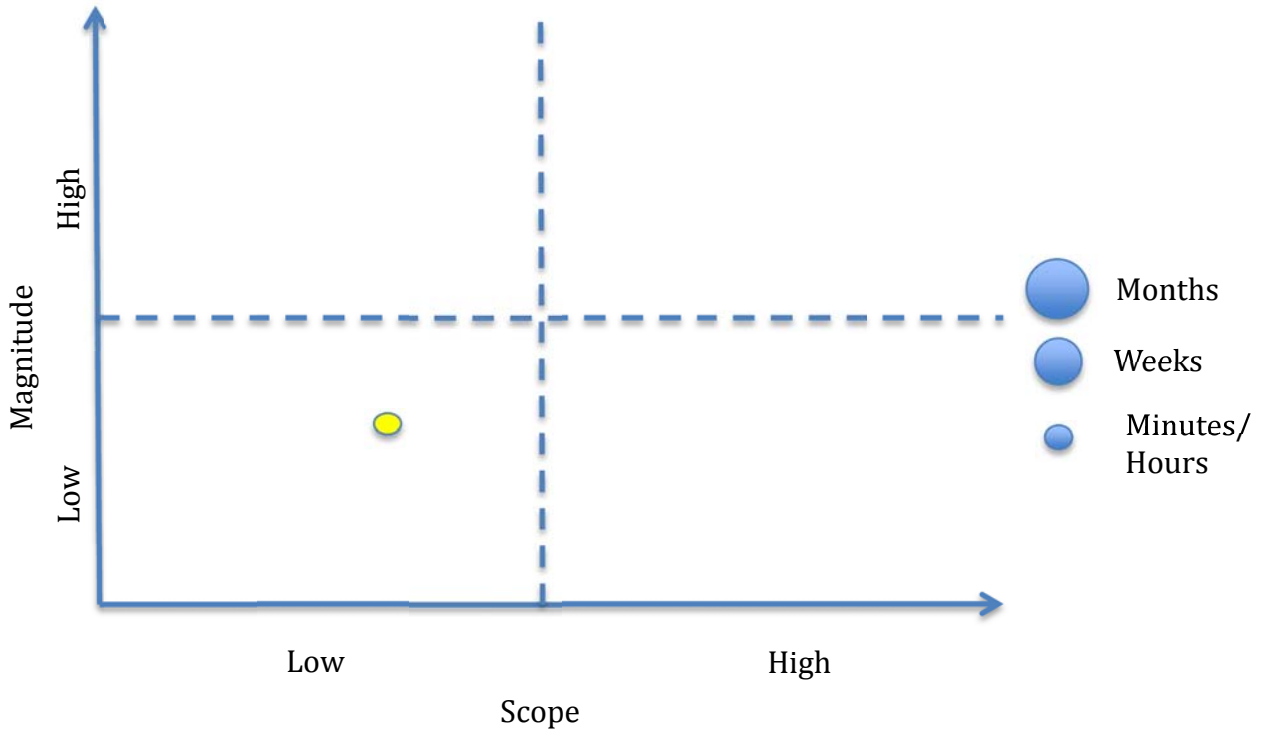


Figure 5: CDI Estimate for Disruptive Effect of the Estonian DDoS Event

[24] Akamai, "Q2 2014 Global DDoS Attack Stats", http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2-quarterly-trends-infographic.html, Akamai, 2014.

Internal communication disruption: Disruption of internal operations through a denial of service

While external DDoS events target a network's ability to communicate with external users, disruptive events that deny internal network communications can have a far wider impact on the functions of the targeted organization. A disruptive event that targets the *internal operations* of a network, thereby preventing employees from accessing e-mail, files, or other network services, can lead to reductions in an organization's output, productivity, and possibly threaten long-term market share for its products and services. If an attacker has access to internal systems and denies users the ability to communicate between their computers and corporate systems (e.g., e-mail, data servers) then operations can quickly grind to a halt. This type of event requires an attacker to have secured access to an internal system and, in order to achieve maximum effect, likely requires access to core networking infrastructure internal to the organization. While an attacker might aim to disrupt the greatest number of computer systems possible in an organization's network, such an effect can be enabled through the execution of an attack against a few, highly important network devices. Characteristics of internal communications disruption events include:

- attackers leverage internal network access to deny employee or user access to files and services (e.g., e-mail) but don't affect the underlying data or equipment;
- large numbers of computers can be rendered useless, as essential services (e.g., e-mail) are inaccessible; and
- attackers are able to lock out system administrators from the network infrastructure, leading to significant delays in reconstituting normal operations.

While not as prevalent as DDoS events, internal denial of service events can and have occurred, usually with much greater effect. One such event impacted the operations of several financial and media organizations. On March 20, 2013, three South Korean television stations and several banks suffered problems with their internal computer systems, along with problems interacting with ATMs and mobile payment systems.[25] The attack consisted of several well-orchestrated events, including an external DDoS, deletion of data, and blocking of traffic between internal systems.[26] While denying access to external websites and deleting data from internal computers (discussed in the next section) is concerning, blocking information between internal systems can significantly magnify the impact an attacker has by denying access to corporate systems that serve an important function. In the case of the South Korean event, employees were unable to access internal files, e-mail access was denied for workers, and ATMs were unable to communicate with bank internal systems, thereby denying bank customers' access to monies in their accounts.

[25] Sang-hun, C "Computer Networks in South Korea are Paralayzed in Cyberattacks", http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html, New York Times, March 2013; Krebs, "The case for North Korea's role in Sony hack", http://krebsonsecurity.com/tag/dark-seoul/, Krebs Security Blog, December 2014.

[26] Symantec, "Four Years of Dark Seoul Cyberattacks Against South Korea Continue on Anniversary of Korean War", http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war, Symantec Security Blog, June 2013.

The scope of these types of events tends to be fairly large as network traffic is impeded through the attacker's compromise of core networking systems. While an attacker might only maintain access to a few computer systems in a larger network, if those systems are central in importance to a network's function (e.g., the router) then the scope of the disruption is greatly magnified. For example, if an attacker maintains access to a core router or switch in an organization's network, he now has the ability to disable computer packets from traversing through that system. While users of other computer systems are still able to access their local files and programs, any attempt to access systems distributed in that network or on the internet are prevented (e.g., websites on the internet or files on a file server). In the Korean disruptive event, only a handful of important systems including domain controllers, e-mail servers, and file servers were compromised by the attacker, but disruptions to those systems impacted employees and customers who were unable to access files, e-mail, and even cash from their accounts.[27] Therefore, these types of cyber events tend to have a larger scope than a simple compromise of a social media account or even a large-scale DDoS of a webserver.

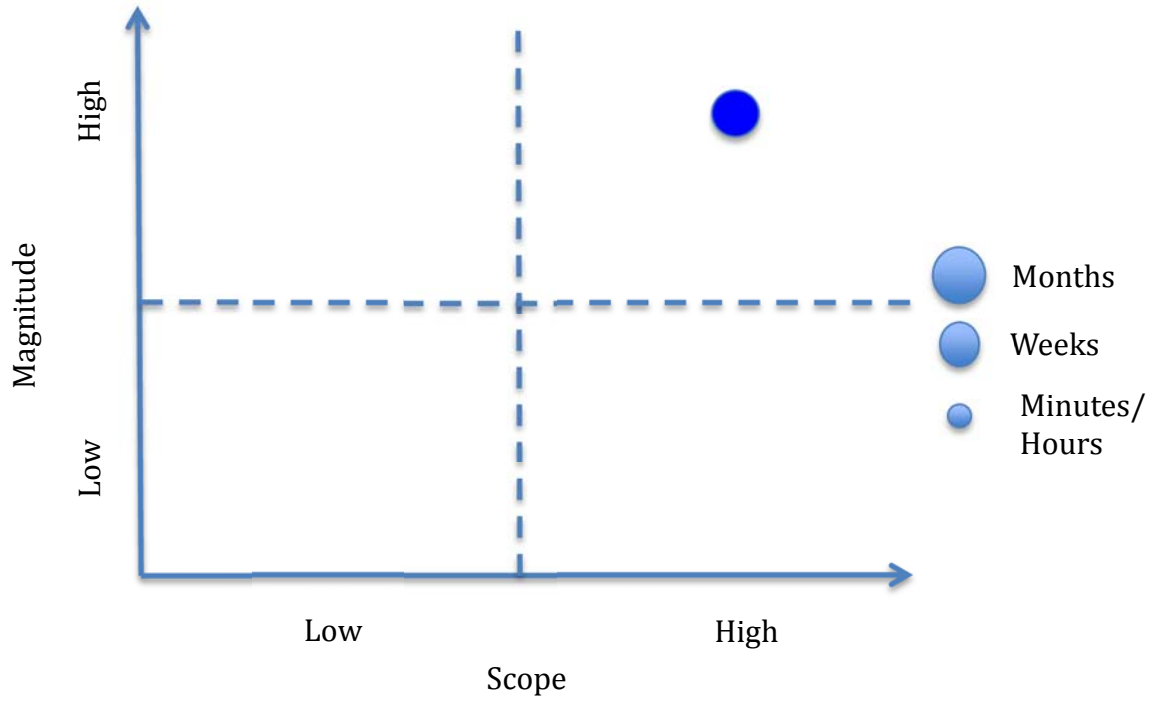
The magnitude of these types of events tends to range from moderate to severe, as attackers leverage access to internal network devices to push disruptions across the organization's operations. While information on end-host computers are not deleted or destroyed, the inability to access data from internal and external sources prevents employees from accessing needed information or in some cases disrupts the control systems of manufacturing processes all together. As the attacker's objective is to control central network systems, the secondary effect often leads to large numbers of internal computers unable to access vital corporate systems, including access to e-mail, files, or the internet.[28] In large organizations that centralize control systems for inventory or manufacturing systems, denying computers the ability to communicate with one another can cause the shut down of production all together. In the case of the Korean event, the inability of ATM machines to communicate with bank servers precluded customers' withdrawing cash.

Internal disruption of service events tend to last longer than those that originate from external sources. While DDoS events can often be filtered by upstream Internet Service Providers (ISP) or by system administrators, internal denial of service events are often more difficult to address, as the devices causing the disruption are both internal and under the control of the attacker. Often, the account passwords are changed, locking out IT personnel and making it difficult for the system administrator to regain control and recover. This type of disruptive event can take days, weeks, and sometimes months to fully recover. In Korea, system administrators spent days wrestling control back of their internal systems and spent months addressing the long-term impacts of the disruptive event.[29]

Leveraging our analytic framework to the events surrounding the Korean banks, we find that the scope of the event was high, as several key network appliances (file shares, e-mail, etc) were impacted. Further, the magnitude of the event was high as employees were not able to access files and e-mail, and customers were unable to withdraw funds. Lastly, while the event was

[27] Krebs, "The case for North Korea's role in Sony hack", http://krebsonsecurity.com/tag/dark-seoul/, Krebs Security Blog, December 2014.
[28] Ibid
[29] Ibid

mainly addressed in weeks, it did have residual impacts that carried on for months. We can plot this event noting that its overall disruptive effect to the intended target was high in scope and magnitude and was resolved over a period of weeks.



Data attack: Disruption of internal operations through internal multi-point deletion, encryption of user data and destruction of underlying systems

While internal denial of service cyber events leverage small numbers of key systems to disrupt the flow of information between computers with the intent to deny network users access to critical systems, some attackers want to move beyond simply denying access to information and to seek the destruction of the data itself. An attack that directly aims to destroy data or the supporting computer systems themselves in an attempt to permanently disrupt the organization's operations is our fourth type of disruptive event. To affect this type of disruption, an attacker leverages network infrastructure to push malicious code across a large swath of computers to simultaneously delete or encrypt files, remove the operating systems of end-hosts, modify firmware, and, in some cases, attempt to destroy computer hardware itself. To execute this type of event, an attacker would require access to internal networks and the means to deploy and execute code simultaneously across the organization in an attempt to maximize the impact of his actions. Characteristics of data attack events include:

- attackers leverage internal access to networks to destroy data and underlying computer systems not simply denying access;

- the duration of disruptive event is longer as network administrators require time to recover data and replace hardware; and
- the recovery of all data lost is not guaranteed.

In November 2014, the Sony Corporation experienced a severe disruptive event when large portions of its network was taken down and made inoperable.[30] First disclosed on a Reddit posting, the event deleted most of the organization's computers' system and user files.[31] An organization known as the "Guardians of the Peace" (GoP). with suspected ties to the North Korean government, was implicated in the attack.[32] The event combined different tactics: stealing possibly 100 terabytes of data, including email and files, in an attempt to embarrass officials; deletion and encryption of system files from almost 7,000 end-host machines; and compromise of core network appliances, including the mail server and file shares, to help propagate the attack tool set.[33] The company was left without use of e-mail, voicemail, or access to files resident on its computers.[34] The use of multiple techniques to access, propagate, and execute the disruptive event impeded operations at Sony for months.[35]

During a data attack, the scope of encryption and deletion varies from a single computer to most of the end hosts resident in a network. Criminals who leverage encryption to demand payment in exchange for returning data to the user often deploy a single-use disruptive payload. So-called ransomware is often used with targets of opportunity rather than as part of a deliberate campaign. However, attackers can leverage deep access in a target network to push their malicious code to as many computers as possible and then synchronize their execution to elicit maximum effect. In the case of the Sony event, the GoP modified thousands of computers and encrypted contents across most of the corporate network. This allowed the GoP to significantly impact the productivity of thousands of company employees.

The magnitude of encryption or deletion events vary based on the number and types of computers impacted by attackers. Whereas denying access to files on an email server can cause a temporary problem, it also has the possibility of permanently destroying data or making the underlying computer system inoperable.[36] In the Sony case, the loss of local files across thousands of targeted machines, along with the intentional encryption of file shares dramatically

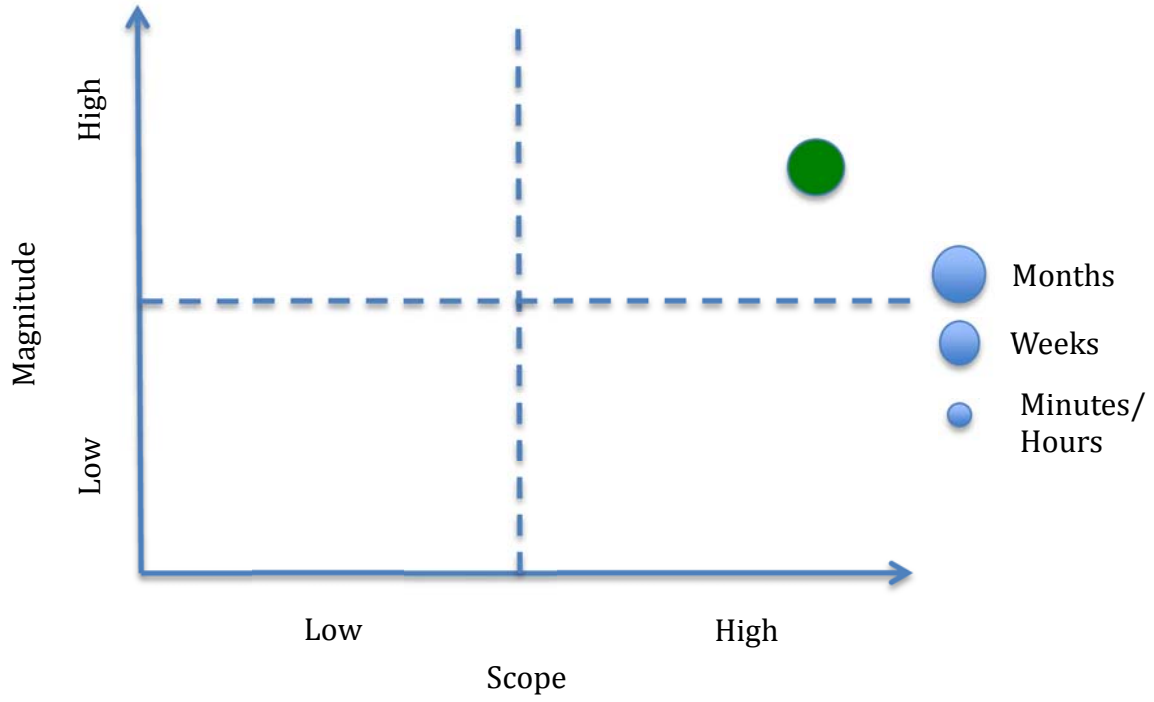
---

[30] Infosec Institute, "Cyber attack on Sony Pictures is much more than a data breach", http://resources.infosecinstitute.com/cyber-attack-sony-pictures-much-data-breach/, Infosec Institute, December 2014.
[31] Ibid
[32] Finkle, J "FBI warns of destructive malware in wake of Sony attack", http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202, Reuters, December 2014.
[33] http://www.businessinsider.com/the-sony-hackers -still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12; Cieply and Barnes "Sony Cyberattacks, First a Nuisance, Swiftly Grew into a Firestorm", http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0, New York Times, December 2014.
[34] Ibid
[35] Pagliery, J "What caused the Sony hack: What we know now", http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/, CNN, December 2014.
[36] Malware Bytes "Cryptolocker Ransomware: What you need to know", https://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/, Malware Bytes, October 2013.

impacted the ability of employees to work. In many cases, employees were reduced to working on whiteboards for weeks.[37]

This event type is often marked by significant delays in return to normal operations. An encrypted disc can be unrecoverable, and the destructive effects to the underlying firmware or hard drive can require significant equipment upgrades.[38] The effect is to push recovery times beyond a few days to months. Reports from the Sony attack indicated that operations were seriously impacted for months, with residual effects lasting longer.[39] The duration of these types of events is driven by both the loss of data through encryption or deletion, and physical damage to the underlying hardware.

The events surrounding the attack against the Sony Corporation demonstrate the potential width of scope and magnitude of damage. In both dimensions, this attack would rate as "high," as thousands of computers were left inoperable; the production of movies, however, did not appear to be directly impacted. The duration of this event can be thought of in terms of at least a couple of months at the end of 2014. We can plot this event visually.



[37] Lee, T " The Sony hack: how it happened, who is responsible, and what we have learned", http://www.vox.com/2014/12/14/7387945/sony-hack-explained, Vox, December 2014.
[38] Malware Bytes "Cryptolocker Ransomware: What you need to know", https://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/, Malware Bytes, October 2013.
[39] Pagliery, J "What caused the Sony hack: What we know now", http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/, CNN, December 2014.

Equipment attack: Disruption through critical infrastructure and control networks

Thus far our discussions have primarily dealt with disruptive cyber events that target the communications path or the data residing on computer systems. While denying access to websites, file servers, or even the data itself can severely disrupt an organization's operations, the ability to remotely modify physical equipment such that it is rendered useless represents a significant escalation. Use of network access to destroy physical equipment demonstrates an ability to cross a boundary between the cyber and physical worlds, highlighting a vulnerability to the underlying systems that support modern life. While rare, these types of events are often seen by countries as acts of sabotage and could be met with retaliation by conventional means. Executions of these attacks usually require deep access to target networks, familiarity with underlying control systems, and significant resources.[40] The characteristics of equipment attack events include:

- attackers leverage internal access to networks to modify control systems;
- the impact to physical equipment can have sustained effect on the production of products; and
- the resulting impact of tends to be long, as physical equipment needs to be replaced and changes need to be made to the underlying network infrastructure.

In December 2014, a German Federal Office for Information Security report noted the infiltration and destruction of equipment at one of the country's steel mills.[41] The event, noted to be only the second confirmed industrial control system attack, appeared to leverage remote access by an unknown actor in the corporate network to modify the control systems, causing a blast furnace to overheat and eventually be destroyed.[42] While technical details concerning the event have yet to be released by the German government, the physical destruction of plant equipment was estimated to impact the ability of the organization to maintain levels of production prior to the event. Replacement of damaged equipment is likely to take months due to the need to remove and replace large pieces of machinery.[43]

The scope of this type of event is slightly different than some of the other events we have discussed earlier. In previous examples, we looked primarily at the importance of computer systems to the operations of a network and/or to the number of end-hosts impacted. In this type of event, the damage migrates outside of a corporate network to the physical environment. The scope might be more limited than an internal communications disruption or data destruction event, as fewer central network nodes are impacted. In the case of the disruption of the German steel mill, the corporate network was not disrupted (although it was used as an access channel), but the physical capital connected to that network was impacted.

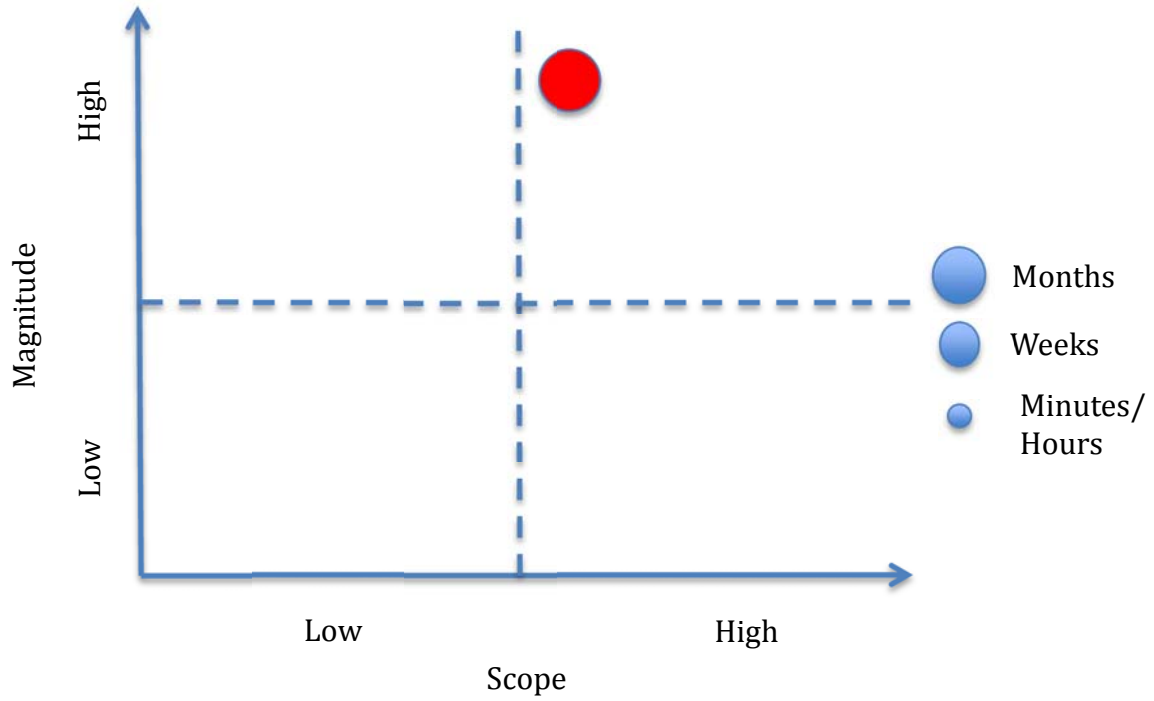
---

[40] Falliere, Murchu,and Chien " W32.Stuxnet. Dossier" http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011.
[41] BBC, "Hack attack causes massive damage at steel works", http://www.bbc.com/news/technology-30575104, BBC, December 2014.
[42] SANS Institute, "ICS CP/PE Case study Paper "German Steel Mill Attack", https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf, SANS Institute, December 2014.
[43] Ibid

The magnitude of an equipment attack event is directly related to the productive capacity of the number and importance of equipment destroyed or impeded. For example, disruption to a control system that manages the dimming of lights in an office is not as impactful as the destruction of large power generators at a local power utility, which affects the level of power on the grid. While an internal communications disruption or data attack event causes production outages through the indirect effect of denying access to communications or data, an equipment attack event destroys the factor of production directly. In the case of the German steel mill, the magnitude of the event is a function of the productive value of the furnace that was destroyed. News reports have indicated that the destroyed furnace was directly involved in the operations of the mill and can be assumed to be highly valuable to the organization.

The duration of an equipment attack event is likely to be longer than other types of disruptive attacks, as physical equipment is rendered inoperable. While some physical equipment can be easily replaced, in some cases, specialty equipment takes months if not years to fully replace. In the German steel mill example, the destruction of a blast furnace required the removal of the damaged capital, shipment of new equipment, and time by mechanics and operators to install and bring online a new furnace. Disruptive events that target the equipment that underpin large-scale manufacturing, utilities, or service provision will no doubt take longer to recover from than simple message manipulation or external service disruption events, and most likely longer than internal communications disruption and IV attacks.

Disruptive events targeting physical infrastructure or machinery are often seen as the most dangerous type of disruptive event. Leveraging the approach laid out in this paper, we find that the events surrounding the attack against the German Steel Mill are higher in scope than a DDoS event, but may not be as great as what we found with the attack against the Sony Corporation. However, as the attacker was able to infiltrate the control systems of a furnace vital to the production process, the magnitude of the event may be rated as high. Lastly, the duration of this event is likely to extend to several months as new equipment must be ordered and installed. We can plot this event with a medium to high scope along with a high magnitude and a duration that extends several months.



Comparative analysis of differing cyber disruptive events and segmenting risk

In the preceding sections we explored five different types of cyber disruptive events along three dimensions of analysis. This approach enabled us to review examples of disruptive events and to qualitatively assess the scope, magnitude, and duration of each event. The table below captures the assessment of each along all three lines of analysis. Pivoting among three dimensions of analysis provides better context from which to comment on disruptive events. As the approach in this paper demonstrates, not all cyber events are equal. While some have the potential to inflict significant effects on the operations of an organization, others are merely nuisances that are easily remedied.

Disruption Type	Scope	Magnitude	Duration
Message Manipulation ISIL Account Hijack	Low (External Account)	*Insignificant-Low*	*< 1 Hour*
External Service Disruption Estonian DDoS	*Low (Webservers)*	*Low*	*Hours to Days*
Internal Communications Disruption Dark Seoul DoS	*Moderate (Dozens of Central Computers Systems)*	*Moderate to High*	*Weeks to Months*
Data Attack Sony Corporation	*High (Thousands of Computers)*	*High*	*Months (1-4)*
Equipment Attack German Steel Mill	*Moderate-High (Small Number of Key Controllers of Physical Equipment)*	*High*	*Months (6+)*

Table 1: Comparative Table of Disruptive Cyber Events

We can also visually represent the disruptive effect by plotting each event along two axes. In the figure below, we plot each of the examples along two axis representing the scope and magnitude of the cyber disruption. The duration of each event is denoted by the size of the event marker. Of the five events, the compromise of the CENTCOM social media presence and the DDoS of Estonian Government websites are small in scale and carry a limited magnitude in the operations of the target. Further, the duration of both events is largely measured in hours thereby having a limited total disruptive effect. Conversely, the attacks against the Sony Corporation, the "Dark Seoul" events, and the attack against the German steel mill significantly impact the target organizations. The larger scope, higher levels of magnitude, and longer duration make these events more disruptive than the previous two. This approach visualizes the total disruptive effect on the targeted organization for each cyber event by highlighting scope, magnitude, and duration.

Comparative analysis among cyber Events

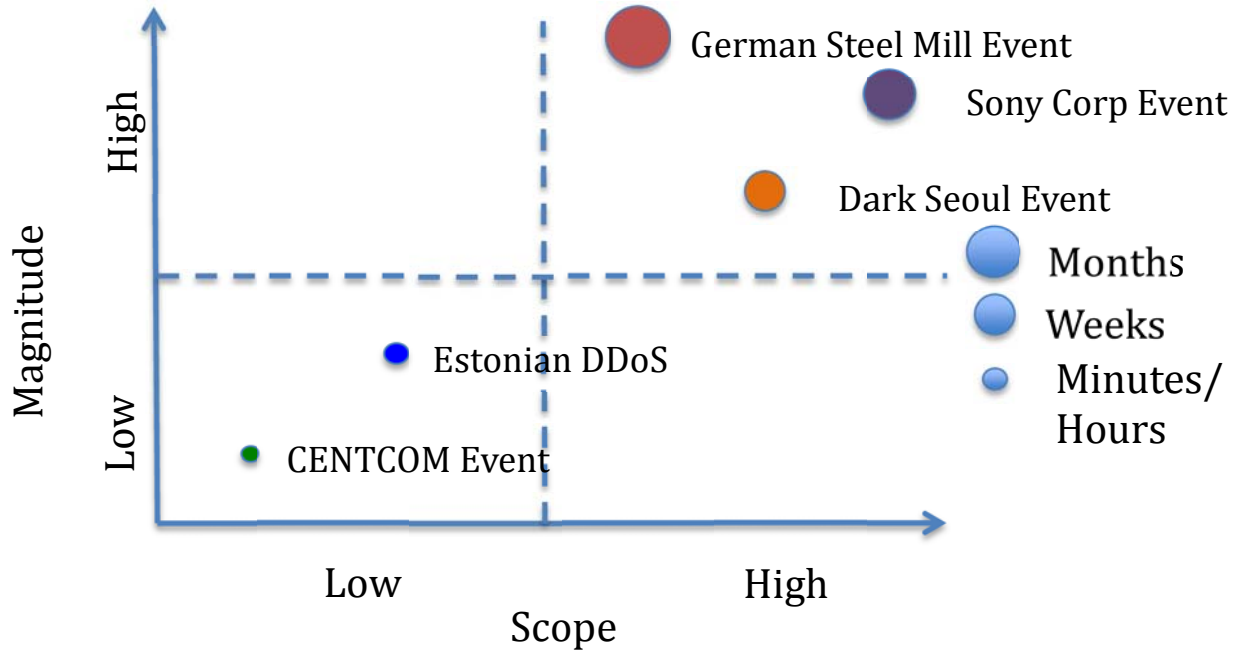


Figure 6: Comparative View of Disruptive Cyber Events

By breaking down events into the 5 categories identified in this paper and leveraging the CDI to assess the magnitude of events, we develop a means by which IT professionals, managers, and public officials can think through specific disruption scenarios. Organizations that have adopted specific security measures, including the provision of firewalls, intrusion detection systems, or two-factor authentication, can assess how those efforts may or may not reduce the risk of specific event types from occurring. For example, an organization might find that while it has robust protections and filtering capabilities in place to minimize its exposure to an external service disruption event (DDoS), it fails to protect its manufacturing systems from an equipment attack event. Organizations are able to take a single view of their operations and differentiate between their vulnerability to different types of events. Figure 7 shows this differentiation and breaks down assessed vulnerability by each of the categories discussed in this paper.

Event Type	Assessed Vulnerability
Message Manipulation	High
External Service Disruption	Low
Internal Communications Disruption	Medium
Data Attack	High
Equipment Attack	High

Figure 7: Representative Organization's Self-Assessment

Protecting against all categories will require leveraging different defensive strategies, including the installation of hardware and software defense systems, changing network topologies, and limiting access to the most sensitive systems in the organization. By breaking down threats to a system into categories, an organization is able to develop a more comprehensive assessment of its vulnerabilities to a complete range of disruptive scenarios.

Estimating the social consequences of disruptive cyber events

While organizations can leverage the framework identified in this paper, this approach has limits. The most apparent is its inability to capture the broader social consequences of specific disruptions, a topic that is of great interest to policy makers. Visually representing disruptive effects from an organization's perspective is useful, however, it does not give policy makers an understanding of the relative effect each type of event has on society at large. Disruptive events aimed at critical infrastructure or at systemically important institutions not only affect the operating organization, they also induce additional impacts on dependent industries. For example, the destruction of production equipment at a large tire manufacturing plant could delay the production of cars at another company. In extreme situations, the loss of productive capacity might lead to the temporary layoff of employees, reducing household incomes in the locality and also tax revenues. The output reduction at the tire manufacturer might also lead to less demand for raw materials thereby impacting suppliers. These secondary effects are the broader social impacts that policy makers have to understand in order to assess which industries impose large social costs and merit comprehensive oversight in implementing cyber defenses.

By slightly modifying the CDI framework, a policy maker can assess the social disruption of a cyber event. If two separate organizations are the victim of a significant disruptive cyber event that affects their production systems, their self-assessed CDI might be similar (see top two graphs in Figure 8). Yet for a policy maker, it is insufficient to simply know the impact of the events on the organization itself; additional questions would remain concerning the broader consequences of the events on the whole of society. For example, if the first organization was a factory that manufactured toy dolls and the second was a power generation plant, a different societal impact could be expected based on the connections between the affected organizations and other entities. The doll manufacturer is unlikely to have significant connections to other firms, while a power plant could have significant linkages. In other words, the attack on the power plant is likely to generate a larger social cost.

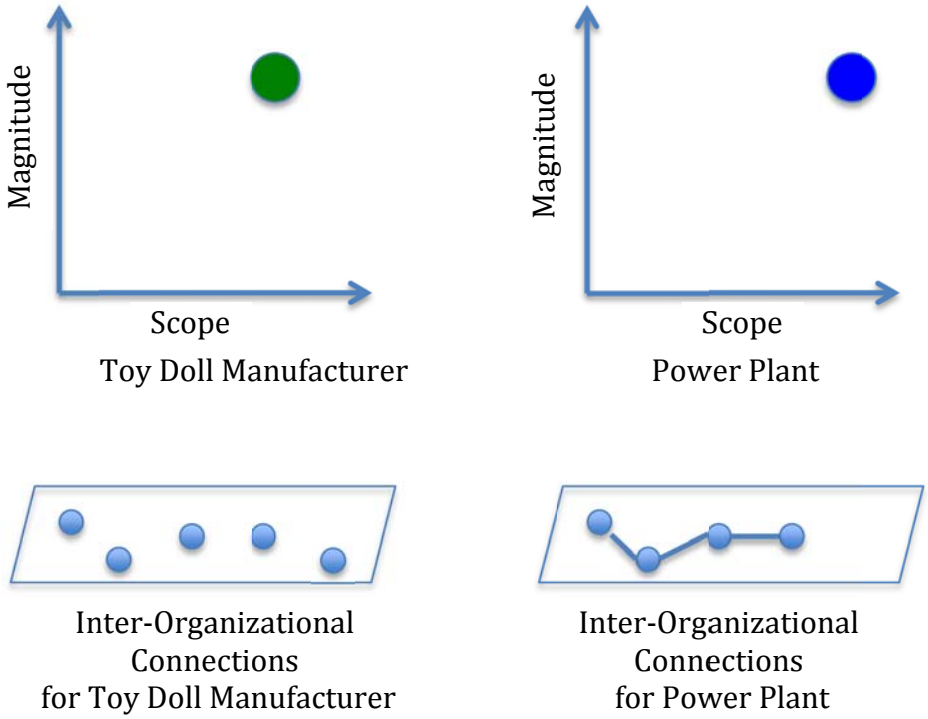


Figure 8: Inter-Organizational Connections and Cyber Disruption

We can visualize this difference by leveraging the CDI and charting the magnitude, scope, and duration of the event relative to the broader impact it has on society. We can start by using the construct discussed earlier and make small changes to account for the secondary impacts the disruption would likely have on the entire production chain. The scope of the event would no longer be the set of computer devices in the immediate organization's network, but would broaden to include the number and importance of *additional* organizations affected by the disruptive event. We would assess this broader scope by examining the topology of the interconnected organizations and the centrality of the firms in that production chain. The measure of the event's magnitude should take into account the change in output at every impacted organization in that topology. Output reductions relative to normal operations, coupled with the broadly defined scope would provide a context for understanding the event's full effect throughout that production chain. Lastly, measuring the duration of the event requires examining the duration of the disruption throughout all of the affected organizations. Mathematically this relationship is represented with the following equation:

$$SDI = \sum_{t}^{m} \sum_{f}^{n} C_f \left(1 - \frac{Y_{f,t+m}}{Y_{f,t}}\right)$$

SDI = Social Disruption Index
t= time period
f= Firms connect to the disruption at the targeted firm
Y = Output of Firm
C = Centrality Score of Firm in Production Chain

In the case where a power plant and doll manufacturer were targeted, the disruptive effect on each firm itself was estimated, using the CDI framework, to be significant; applying an additional layer of analysis that includes the interconnections between organizations, we can differentiate between the two events further, demonstrating that one of the attacks is of greater societal significance than the other. The figure below reassesses both events utilizing this new construct. Since the power plant has significantly more interconnections with other organizations than the doll manufacturer, the overall disruptive effect to society is higher. Figure 9 highlights this difference with scope, magnitude, and duration of the attack on the power plant dwarfing the effect of the attack on the doll manufacturer. While both organizations experienced a significant disruptive attack, the one with the larger social impact is the event at the power plant, whose loss of power production cascades through its connections to other organizations.

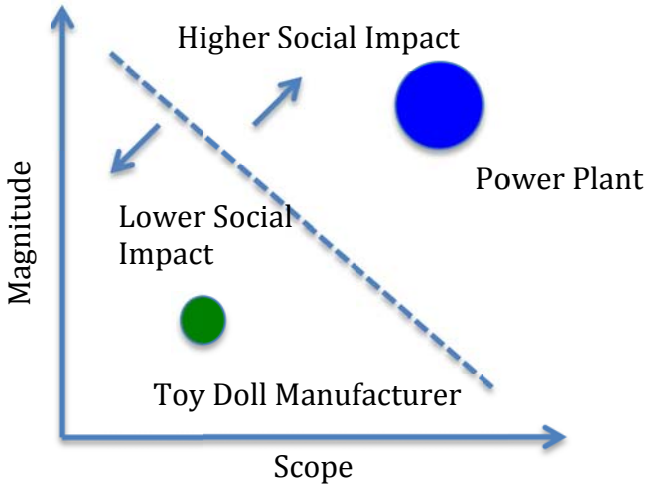


Figure 9: Social Disruption of two Cyber Events

The SDI scale helps to differentiate the events and clarify which represent a clear threat to broader society. Cyber events that are high in scope and magnitude because of their significant linkages in society are likely to demand greater oversight by public officials, whereas broad-based and voluntary measures might be adequate for the vast majority of other threats.

Policy makers confront an increasing number and diversity of cyber threats. This has generated significant awareness of the general issues, but the lack of a way to classify, measure, and assess cyber threats has limited the policy makers' abilities to craft comprehensive frameworks that differentiate between threats. This paper presented a taxonomy of cyber disruption, providing a technique to assess the size of cyber disruption, and finally a means by which government officials can assess the broader social significance of a cyber event. The resulting analysis should help organizations direct scarce resources to minimize their vulnerability to disruptive events and provide public officials a means of assessing which types of events pose the most significant risks to society. Identifying the most critical industries and the disruptive technique that can be employed against them should assist in minimizing vulnerabilities—to both the organizations and society at large.

About the Author

Charles Harry is vice president for cyber and analytic solutions at Blackpoint Technologies, LLC, and a Research Scholar at the Center for International and Security Studies at Maryland.

References

Akamai, "Q2 2014 Global DDoS Attack Stats", http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2-quarterly-trends-infographic.html, Akamai, 2014.

Anderson, Ross, "Why Information Security is Hard - an Economic Perspective," Proceedings of the 17th Annual Computer Security Applications Conference, 2001.

BBC, "Hack attack causes massive damage at steel works", http://www.bbc.com/news/technology-30575104, BBC, December 2014.

Cieply and Barnes "Sony Cyberattacks, First a Nuisance, Swiftly Grew into a Firestorm", http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0, New York Times, December 2014.

Citizenlab "China's Great Cannon", https://citizenlab.org/2015/04/chinas-great-cannon/, Citizenlab Blog, April 2015.

CSIS. "Cyber Legislation," CSIS Technology and Public Policy Blog, June 17, 2011.

Critical Infrastructure Act of 2002, U.S Congress, November 2002.

Department of Defense Strategy for Operating in Cyberspace, U.S. Department of Defense, July 2011.

Dunn, J "Asian Datacentre hit by massive 334 Gbps DDoS Attack, Arbor Networks reveals", http://www.techworld.com/news/security/asian-datacentre-hit-by-massive-334gbps-ddos-attack-arbor-networks-reveals-3609764/, Techworld, April 2015.

E.O 13636 Improving Critical Infrastructure Cybersecurity, Executive Office of the President, February 2013.

E.O 13691 Promoting Private Sector Cybersecurity Information Sharing, Executive Office of the President, February 2013.

Falliere, Murchu,and Chien " W32.Stuxnet. Dossier" http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011.

Finkle, J "FBI warns of destructive malware in wake of Sony attack", http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202, Reuters, December 2014.

Foster, P " US CENTCOM Twitter account hacked by Islamic State", http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11341057/US-military-twitter-account-hacked-by-Isil.html, The Telegraph, January 2015.

Friedman, Allan, "Economic and Policy Frameworks for Cyber Security Risks" Brookings, July 2011.

Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73.

Gallagher, S "Inside the wiper malware that brought Sony Pictures to its knees", Ars Technica, December 2014.

Gallagher, S " Your Hardrive will self destruct at 2pm: Inside the South Korean Cyberattack", "http://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/, Ars Technica, March 2013.

Goodman, Seymour E. and Herbert Lin, National Research Council (U.S.), Committee on Improving Cybersecurity Research in the United States, *Toward a Safer and more Secure Cyberspace*, National Academies Press, 2007.

Infosec Institute, "Cyber attack on Sony Pictures is much more than a data breach", http://resources.infosecinstitute.com/cyber-attack-sony-pictures-much-data-breach/, Infosec Institute, December 2014.

Lamothe, D "U.S military social media accounts apparently hacked by Islamic State sympathizers" , http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/, Washington Post, January 2015.

Lee, T " The Sony hack: how it happened, who is responsible, and what we have learned", http://www.vox.com/2014/12/14/7387945/sony-hack-explained, Vox, December 2014.

Lieberman, Joe, Susan Collins, and Tom Carper, "A gold standard in cyber- defense," *The Washington Post*, July 7, 2011. http://www.washingtonpost.com/opinions/a-gold-standard-in-cyber- defense/2011/07/01/gIQAjsZk2H_story.html

Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (July 2013), pp. 365–404

Malware Bytes "Cryptolocker Ransomware: What you need to know", https://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/, Malware Bytes, October 2013.

National Strategy for Trusted Identities in Cyberspace, Executive Office of the President, April 2011.

Pagliery, J "What caused the Sony hack: What we know now", http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/, CNN, December 2014.

Perlroth, N, “Cyberattack that hit Target a widespread threat to customers” http://www.bostonglobe.com/business/2014/08/22/cyberattack-that-hit-target-affecting-businesses/AmsccErTlI4vLhQpUfSorL/story.html, Boston Gloge, August 2014.

Sang-hun, C “Computer Networks in South Korea are Paralayzed in Cyberattacks”, http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html, New York Times, March 2013.

SANS Institute, “ICS CP/PE Case study Paper “German Steel Mill Attack”, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf, SANS Institute, December 2014.

Soergel, A “53 million email addresses stolen in Home Depot Hack”, http://www.usnews.com/news/newsgram/articles/2014/11/07/53-million-customer-email-addresses-leaked-in-home-depot-hack , US News and World Repot , November 2014.

Symantec, “Four Years of Dark Seoul Cyberattacks Against South Korea Continue on Anniversary of Korean War”, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war, Symantec Security Blog, June 2013.

Symantec, “The Shamoon Attacks” , Symantec Blog 2012 http://www.symantec.com/connect/blogs/shamoon-attacks

Traynor, I “Russia accused of unleashing cyberwar to disable Estonia ,http://www.theguardian.com/world/2007/may/17/topstories3.russia, Guardian, May 2007.

Security and Privacy Controls for Federal Information Systems and Organizations – Special Publication 800-53, National Institute of Standards and Technology, April 2013.

Valeriano and Maness, “The Fog of Cyberwar: Why the Threat Doesn’t Live Up to the Hype,” *Foreign Affairs*, November 21, 2012, https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar

Valeriano and Maness, “The Dynamics of Cyber Conoict between Rival Antagonists, 2001–2011,” *Journal of Peace Research*, Vol. 51, No. 3 (May 2014), pp. 347–360.

Appendix: Defining the Cyber Disruption Index

Scope: Understanding the Topology of Disruption

The scope of a disruptive cyber event is a best understood through the topology of the impacted network and the range of effects on it. The scope of any disruptive cyber event is a function between the number of devices impacted by the event and the importance of those nodes to the overall network. An event that destroys data across 30,000 computers in a company's internal network might have a larger disruptive effect than temporarily making an external webserver unavailable; yet the disruption of a single core routing device that handles networking traffic across an entire topology can affect the operations of thousands of other devices due simply to its relationship with other end-hosts. The balance between numbers and importance demonstrates some of the complexities associated with measuring the scope of an event.

Topology: Counting the number of affected nodes in a network

To understand a disruptive event's topology, and the impact they can have, it is useful to apply basic graph theory as a means to visualize and discuss how nodes relate to one another. We can visualize a simple computer network as a Graph (G) with J vertices (e.g. nodes) and E edges (e.g. lines). In a simple graph, the vertices can represent networking equipment or end host machines (e.g. personal computers), while the edges represent the logical connection between these devices. This representation enables us to easily visualize a network, its connections, layout, and relation to the broader Internet. In the figure below, I lay out a very simple network with 9 vertices, and where one is directly connected to the Internet (vertex J).

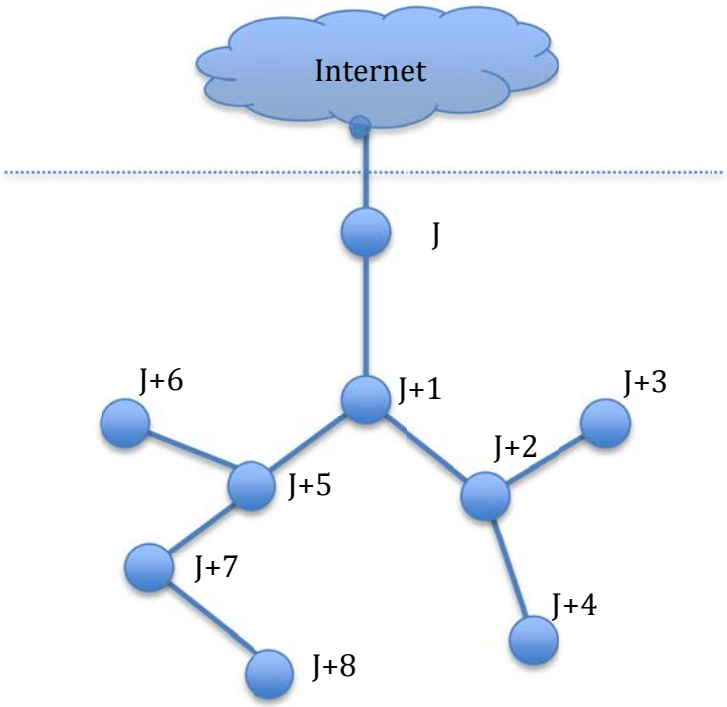


Figure 10: Representative Topology of a Network

Our first element of analysis is simply a count of the number of vertices impacted by a disruptive event. If we evaluate a hypothetical disruptive event that impacts vertices J, J+1, and J+2 on the topology in Figure 1 then we can quick determine that 3 nodes in a topology of 9 was impacted or roughly 33% of the network's topology was affected. A large scale event that disables the functions of 33% of a network's devices will no doubt have a significant effect on a firm's operations.

Yet while the sheer number of vertices is important the location and connections a vertex maintains can yield even greater disruption to network operations. If all vertices required access to the internet then even disruption to a single node (e.g vertex J) would deny all vertices access to the internet. To understand those relationships, we would need to understand both the importance of impacted vertices have on paths between one point and another (betweenness) in a network as well as for how central (centrality) those nodes are in the network.

Topology: Understanding the importance of a node to a network

Aside from the number of nodes impacted the importance of each node to a network also important to understand. How "central" a vertex is to an affected topology might demonstrate an ability for a disruptive event to segment a network and cutoff other nodes from communicating with each other. For example, a simple visual analysis of Figure 1 would yield a conclusion that node J+8 is less central to the graph G then node J+1. This would imply that a disruptive event that hits only J+8 would have a smaller scope of disruption then if node J+1 were impacted. While it is entirely possible that the productive activities of node J+8 are extremely high[44], the breadth of the disruption is still likely to be smaller due its lower degree of centrality in the network. While there are many measures of centrality in a network, the calculation of Eigenvector centrality[45] is useful to understand the relative importance a specific node has within a network. While the specific calculation of nodal centrality is beyond the scope of this paper, the concept is important as a distinguishing element of the topology of disruption and useful in constructing a measure of scope and for a larger measure of cyber disruption.

Topology: Compiling a Disruptive Event's Scope

There are two fundamental elements in our measurement of the scope of a disruptive cyber event. The number and importance of nodes affected by the actions of a malicious actor help us quantify the range of effect on the targeted network. These concepts can be expressed mathematically with the following equation:

$$Scope\ of\ Event\ = \sum_{j}^{n} C_j I_j$$

$Where$
$C_j = Eigenvector\ centrality\ Score\ for\ node\ j$[46]
$I_j = 1\ where\ node\ j\ is\ impacted\ by\ event, 0\ where\ node\ j\ is\ not\ affected$

[44] A high level of centrality does not imply it is more important than a lower amount, but does indicate a more centralized position in the topology. Discussion of magnitude of impact is handled later in the paper.
[45] Insert citation

The number of nodes affected, their dependent relationships with one another, and the centrality of the nodes affected all contribute to the scope of a disruptive event. While the breadth of a disruptive event is a critical determinant for evaluation, it is closely coupled with the magnitude of the individual impacts for each vertices in a topology, and the subsequent duration of a disruption. In the following section of this paper I address an approach to measure the relative magnitude of disruption on a specific node and its impact to capital deployed by an organization for purposes of production.

Magnitude: How Large is the Disruption?

In the previous section we discussed the scope of a disruptive cyber event including estimating the number, relationships, and position of impacted nodes. However, scope alone is insufficient to categorize the specific types of events faced by firms and governments. To gain a better appreciation of the relative scale of the malicious activity we must be able to ***pair both the scope of the event with the magnitude*** across affected nodes. In principal there are several considerations we must deal with when estimating the magnitude of cyber disruptive event. These might include the effect on the perception of the firm or its brand by the public or the impact to future sales resulting from concerns surrounding the ability of a firm to make good on its commitments. While these considerations are important and have been dealt with by others, fundamentally, the effect of an event must be tied to the ability of an organization to produce a good or service. It is this last estimate of direct impact that this paper addresses.

Magnitude: Defining the central concern of the enterprise

While the magnitude of cyber disruption can be assessed through external measures (e.g effect on stock price), the central concerns surrounding disruptive cyber events are the effects to production and the underlying productive capacity of a firm's technology. While media accounts of basement hackers making there way into networks for the purpose of marking up public accounts or websites, the central concerns of boardrooms and executives must center around the production of goods and services. We might find the following questions asked by senior business leaders:

- How many tons of steel will not be produced because a network is not working?
- How will customers be able to place orders if the company's website is unavailable?
- Can I manage my inventory when my internal systems are unavailable?
- Can I run my operations if my data servers are off line?

These questions go to the heart of concerns regarding disruptive events--Can goods and services be produced and distributed after a disruptive event has occurred? To help frame this problem it is useful to anchor our analysis as part of a firm's production function. Basic microeconomics

[46] Eigenvector Centrality calculation is equal to $C(\alpha,\beta) = \alpha(I - \beta R)^{-1}R1$,
Where: α *is a scaling vector,* β *reflects the extent to which you weight* the centrality people is tied to, R is the adjacency matrix, I is the identity matrix, and 1 is a matrix of all ones.

defines the production of a good as the combination of labor and capital to produce a good. In the case where L is considered units of labor and K is considered units of capital, they are brought together using technology, $\emptyset$, to produce some level of output.

$$Y = \emptyset * f(L, K)$$

If the value of technology ($\emptyset$) is greater than one than the production function exhibits increasing returns to scale, decreasing returns to scale if less than one, and constant returns to scale if equal to one. Yet what if a malicious actor were able to penetrate a computer network that links capital equipment (e.g production robots in a car manufacturer) and shuts down the connection between those pieces of equipment, can technology's contribution to the production function itself be impacted? In the case of a cyber disruption event, I propose that the underlying technology that integrates the factors of production is affected thereby reducing the contribution of technology in the production process and lowering overall output.

Magnitude: Impacting production

Technology is primarily thought to improve efficiencies and to enable labor and capital equipment to work together in an integrated manner to produce goods, but if that technology were disrupted then it can no longer be seen to add to the efficient deployment of the factors of production. In fact the widespread disabling of key network devices or software applications can slow down or completely stop the production process. It follows then as the productive value of technology used by a firm approaches zero, production of a firm's good also approaches zero.

If the technology of a firm prior to an event is defined as $\emptyset$, and the value of technology affect on production after an event is defined as $\emptyset^*$,where $\emptyset > \emptyset *$, then it follows that as $\emptyset^*$falls as a result of a disruptive event then output (Y) itself is reduced. This reduction can be thought of as the aggregated effect of a cyber disruption on the underlying productive capacity of a firm's technology.

$$if\ \emptyset^* < \emptyset \quad \text{it follows that } Y^* < Y$$

While it is easy to tie the aggregated effect of technology to production, the reality is that technology is disaggregated and networked across disparate geographies often consisting of thousands of connections. These interconnections often tie together disparate nodes each with differing contributions to the production of goods and services. In a network consisting of thousands of computing devices the processes required to manufacture or produce a product each have disparate productive topologies that when affected by a malicious cyber event lead to differing impacts. Those changes to the productive capacity of the underlying technology must be addressed to accurately approximate the impact an even has on the firm.

Magnitude: Disaggregating effect of technology on production

Our ability to discern the magnitude of an event is tied to the disruption of the underlying technology that enables the production of a product or service to its customers. If the production

of goods and services are reliant on the underlying technology of the firm, then it follows that in addition to the change in output, it is fundamental for us to identify the relative change in productive capacity of technology employed by a firm. While technology is a broad term captured by a single variable in our generic production function, in modern firms it is likely to capture an interconnected network that allows people to interact with software programs that enable the production of goods. Therefore the productive enabling effect of that network must be accounted for in our estimation of the magnitude of disruption.

So how can the disruptive effect be measured beyond the aggregated impact to the firm's production function? To answer that question it is useful to return to our representative network topology. In the figure below we find a representative figure of a deployed computer network. Each node represents a computer that is linked together, where it is used by a unit of labor to help produce a good or service.

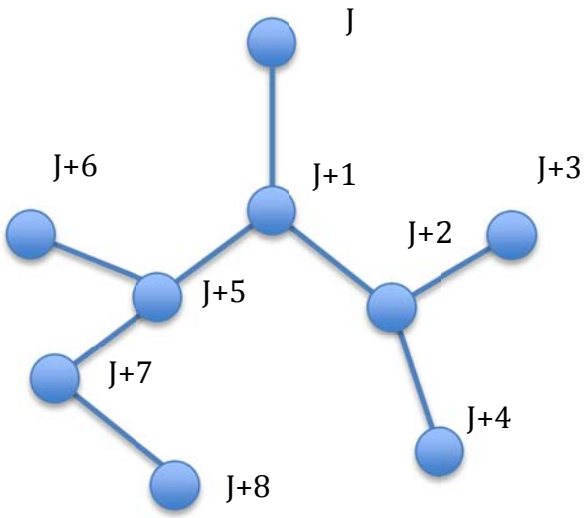


Figure 11: Representative Network

In a world were we do not account for the cyber disruption to our network, the value of a piece of networked computer gear might be equal to the productive effort for that specific node as it simply reflects the productive value to the manufacturing process. An example of this would be the value a industrial control program has in the controlling a manufacturing line. However, if we imagine an event on any of those computers, that productive capacity would be reduced by some amount[47]. While tit might be the case that the computer itself is not damaged, nor the person controlling it is affected, the inability to use the software program to manage the assembly line slows down overall production a good there by reducing productive capacity for that point in the topology. Therefore, let us define that productive effort as the Productive Capacity of Technology (PCT). So for any point of technology on that topology, the PCT is simply the productive effort that node produces which is itself a subset to the overall value technology contributes to production of a good for the firm.

$$\emptyset_j = PCT_j$$

[47] A disruptive event could include a scenario where the computer itself is destroyed, a software application is disabled, or the connection to other nodes is affected.

So for a single node j in our topology, and recalling where ∅ is equal to the overall value of technology used in production, the productive value technology from all nodes j is equal to the overall value of technology applied in the production process. [48]

$$\emptyset \quad = \sum_{j}^{n} \emptyset_j$$

While each node of technology in a topology contains a value of productive capacity for the production of goods, the introduction of a disruptive cyber event highlights a need for us to also account for the cost of that disruption to the application of technology in the firm's production process. Any disruptive event on a node in our network will have some impact that will range from zero to the total value of the PCT for that point in our topology. Therefore let us define a disruptive event on that point of technology (e.g a computer workstation is rendered useless) the Disruptive Effect of Technology (DET). Where for any node j in our topology:

$$0 \leq DET_j \leq PCT_j$$

So for each individual node in our network the true productive contribution it provides to a firm's production is the difference between the overall PCT and the DET. So the share of technology that contributes to overall production for any specific node j, is defined as:

$$\emptyset_j = PCT_j - (E_j * DET_j)$$

Where:
$PCT_j = Productive\ capacity\ of\ Technology\ for\ node\ j$
$E_j = [0,1] Depending\ if\ an\ event\ on\ node\ j\ has\ (1) occured\ or\ has\ not\ (0) occured$
$DET_j = Disruptive\ Effect\ of\ Technology\ for\ node\ j$

We can discern that as when an event occurs (e.g E=1) on a node, and as the value of DET increases, the contribution to a firm's production for this point in our topology approaches zero. As both the impact of the event and the number of nodes impacted by the event grows the larger the impact to the firm's production, as more and more machines are rendered useless. Likewise the disruption to an exceptionally important node (e.g File server or industrial control system) also have a wide ranging effect on the firm's production despite only a small number of nodes impacted.

We are then able to discern the impact of a disruptive cyber event Therefore the cumulative effect of a disruptive event on a topology consisting of nodes, can

[48] While this paper only deals with a simple summation for the productive capacity of each node of technology, more complex interrelationships are likely to exists for differing industries and firms.

During normal operating where no disruptive cyber event has occurred, the full productive capacity of the node can be applied. When a disruptive event occurs however, the productive capacity is reduced by some amount as a direct result of the malicious actors intentions. For example, lets assume a computer at ACME company controls an assembly line's operations utilizing both a custom software application to manage production, but also leveraging an inventory system that is reliant on Internet access. Senior leadership have been told by their IT security team that an disruptive event could occur using a known vulnerability that could impact inventory control systems. That impact would reduce the productive capacity of that single computer by 0.5. During the course of its normal operations a single node j's productive capacity of technology (PCT) is equal to one, and since no event has occurred the value for E at that time is zero. Our the calculation of $\emptyset_j$ is straightforward:

$$\emptyset_j = PCT_j - (E_j * DET_j)$$
$$\emptyset_j = 1 - (0) * 0.5$$
$$\emptyset_j = 1$$

Now assume a malicious actor gained access and denied the ability for node j to reach the internet, such that an operator could not use his computer to access the inventory control system, but still allowed control of the assembly line. While production can continue through control of an assembly line, greater inefficiencies are introduced, as inventory is not properly controlled. This leads to a reduction in productive capacity for the node thereby reducing optimum production for the firm. In an extreme case production is halted until all the systems are brought back on line, but here only a portion of the computer's productive capacity is affected. If we assume then that the normal productive capacity for node j is one, but with a disruptive cyber event (g), the effect on that node is 0.5 we find that the new $\emptyset_j^*$:

$$\emptyset_j^* = PCT_j - (E_j * DET_j)$$
$$\emptyset_j^* = 1 - (1) * (0.5)$$
$$\emptyset_j^* = 0.5$$

Running the same exercise on all affected nodes (e.g the scope of the event) and summing the results and dividing over the baseline $\emptyset_j$ provides us an estimate of the fractional productive capacity for all nodes in the network as compared to the baseline prior to the disruptive cyber event.

$$Fraction\ of\ Productive\ Contribution\ (FPC) = \sum_j^n \frac{\emptyset_j^*}{\emptyset_j}$$

The result of the disruptive cyber event is to reduce the value of $\emptyset$ to $\emptyset^*$ thereby reducing the productive capacity of the deployed technology and disrupting the ability of labor and capital to work together.

$$FPC * \emptyset f(L,K) < \emptyset f(L,K)$$

This reduces the firm's overall output from its optimum baseline capability and provides us with two outputs of a disruptive cyber event: change in productive capacity of technology, and the change in output due to a disruptive cyber event.

$$Fraction\ of\ Productive\ Contribution\ (FPC) = \sum_{j}^{n} \frac{PCT_j - (1) * DET_j}{PCT_j - (0) * DET_j}$$

Reduced to

$$Fraction\ of\ Productive\ Contribution\ (FPC) = \sum_{j}^{n} (1 - \frac{DET_j}{PCT_j})$$

$$Disruptive\ Effect\ Contribution = \sum_{j}^{n} (1 - FPC_j)$$

$$Disruptive\ Effect\ Contribution = \sum_{j}^{n} \frac{DET_j}{PCT_j}$$

Duration: How Long will the Disruption Last?

The duration of a disruptive cyber event is the length of time an action is taken by a malicious actor impacts the operations of an organization. Some events might only disrupt a network device for a few minutes or hours, while others destroy equipment that is either very expensive or hard to procure resulting in a larger impact. For example, distributed denial of service attacks occur thousands of times per day, but are often easily addressed by either Internet Service Providers (ISP) or the company system administrators in a manner of a few hours. Events that attack and destroy industrial equipment can have profound impacts to production as it may take weeks or months to replace damaged equipment.

Calculating an Index for Cyber Disruption

Scope * Magnitude *Duration

$$\boldsymbol{CDI = \sum_{t}^{m} \sum_{j}^{n} C_j \left(\frac{DET_{j,t}}{PCT_{j,t}} \right)}$$

$\boldsymbol{Where}$:

$$C_j = Eigenvector\ Centrality\ score\ for\ node\ J$$
$$DET = Disruptive\ Effect\ of\ Technology$$
$$PCT = Productive\ Capacity\ of\ Technology$$