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

CISSM Policy Brief **April 2017**

Categorizing and Assessing the Severity of Disruptive Cyber Incidents

By Charles Harry and Nancy Gallagher

Executive Summary

Faced with a rapidly growing volume and range of cyber attacks, policymakers and organizational leaders have had difficulty setting priorities, allocating resources, and responding effectively without a standard way to categorize cyber events and estimate their consequences. Presidential Policy Directive 41 laid out the Obama administration's principles for executive branch responses to significant cyber incidents in the public or private sector. But it neither drew important distinctions between different types of cyber incidents, nor gave a standard way to determine where a particular incident falls on its 0-5 point severity scale. This policy brief demonstrates how an analytical framework developed at the Center for International and Security Studies at the University of Maryland (CISSM) can help address these problems. It first differentiates between low-level incidents and more significant cyber events that result in either exploitation of information and/or disruption of operations. It categorizes five types of disruptive events and analyzes 2,030 cyber events in a dataset developed from media sources, showing that cyber exploitation remains more common than disruption, and that most disruptive activity fits into two categories: message manipulation and external denial of service attacks. Finally, the brief offers a standard method to assess the severity of different categories of disruptive attacks against different kinds of organizations based on the scope, magnitude, and duration of the event. This Cyber Disruption Index (CDI) is then applied to survey data on Distributed Denial of Service (DDoS) attacks in the private sector to assess severity within a common category of disruptive events. Of 3,900 cases reported, only 5 events (less than 1% of the DDoS cases) had a combined scope, magnitude, and duration severe enough to be a priority for prevention and potentially warrant government involvement.

Presidential Policy Directive 41 (PPD-41), released in July 2016, laid out the Obama administration's principles for executive branch responses to cyber incidents in the public or private sector based on the severity of the threat posed to public health or safety, national

security, economic security, civil liberties, or public confidence.[1] It represented an important step towards clarifying when the federal government should get involved, which agency should take the lead, and how it should work with other public and private actors, depending on the nature, severity, and target of a cyber attack.

Further action is needed, though, because PPD-41 neither drew important distinctions between different types of cyber incidents nor provided a standard method of ranking them on its 0-5 point severity scale. The schema suggests that judgments about the severity of an incident should be based on the type of actions observed and their intended consequences, as well as their scope and scale. But, if government and private sector personnel must make an ad hoc assessment about severity every time a significant event occurs, confusion will impede the rapid, coordinated response to major incidents that PPD-41 is intended to provide.

The lack of shared cybersecurity terminology and assessment methodology creates other serious problems for public officials, industry leaders, news media, and private individuals concerned about cybersecurity. They have no systematic way to differentiate between cyber events that should be managed as a part of normal business versus those that could seriously disrupt critical operations for an extended period of time. Furthermore, PDD-41's severity scale and reporting requirements assess consequences after an adverse event has occurred, so that scale cannot be used to estimate risks, set priorities, and allocate resources to prevent or mitigate future attacks.

This policy brief offers an analytical framework developed by the Center for International and Security Studies at the University of Maryland (CISSM) that can remedy some of PPD-41's shortcomings. The first section differentiates between low-level incidents and more significant events that result in either exploitation of information and/or disruption of operations. It then analyzes 2,030 cyber events reported by major news outlets from January 2014 through August 2016, finding that cyber exploitation was twice as common as cyber disruption. The second section further separates disruptive events into five categories based on what part of a public or private organization's information technology operations were affected. Of the 668 disruptive events in our dataset, most involved defacement of websites, compromised social media accounts, or distributed denial of service (DDoS) attacks, not attacks on internal communication networks and control systems that are typically most disruptive.

The third section demonstrates how CISSM's three-dimensional cyber disruption index (CDI) can be used by different types of public, private, and non-profit organizations to assess the severity of an actual attack, or to estimate the impact of different types of attacks that could happen in the future. It differentiates significant attacks from trivial incidents by analyzing survey data collected by the security firm Kaspersky Labs about one common category of disruptive events, DDoS attacks. Very few of these DDoS victims experienced a moderate to severe effect, with less than 1% suffering the worst consequences, complete transactional failure over several days to weeks.[2]

[1] Presidential Policy Directive-41 "United States Cyber Incident Coordination," White House, July 26th 2016, https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[2] "Global IT Security Risks Survey 2014 – Distributed Denial of Service (DDoS) Attacks," Kaspersky Labs, https://press.kaspersky.com/files/2014/11/B2B-International-2014-Survey-DDoS-Summary-Report.pdf?_ga=1.258421002.1038056443.1457609677

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

	Observed Actions	Intended Consequence[1]
		Cause physical consequence
	Effect	Damage computer and networking hardware
	Presence	Corrupt or destroy data
		Deny availability to a key system or service
	Engagement	Steal sensitive information
		Commit a financial crime
	Preparation	Nuisance DoS or defacement

PDD-41 Cyber Incident Severity Schema

These findings suggest that the vast majority of cyber events should be viewed by policymakers and the media as nuisance attacks that affected organizations should be able to handle on their own with minimal disruption. Using the CISSM framework can help policymakers develop clearer policies regarding when disruptive cyber attacks against private companies are a public concern, warranting government attention to risk mitigation and incident response. It can also facilitate more productive conversations inside organizations, and between government, industry, academic experts, and the media about cyber security risk management and response.

The Need for More Precise Terminology

Policymakers, security experts, and journalists frequently cite terrifying statistics about the rapid rise in cyber attacks. The headline of a March 2016 *Newsweek* article warned, "U.S. Hit by 77,000 Cyber Attacks in 2015 – a 10 Percent Jump."[3] This statistic vastly underestimated the total number of adverse cyber incidents that occurred in 2015, because the data came from reporting requirements that are mandatory for federal Executive branch civilian agencies, and voluntary or non-applicable for all other users of information technology. The headline also grossly exaggerated the threat because the Federal Information Security Modernization Act of

[3] http://www.newsweek.com/government-cyber-attacks-increase-2015-439206.

2014 (FISMA) defines "cyber incidents" to include "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices."[4] Some events, such as the theft of sensitive information about 22 million people from the Office of Budget Management's personnel records, were very damaging. But most of those 77,000 incidents did not seriously jeopardize "the integrity, confidentiality, or availability of information or an information system," and many caused no harm at all.

Casual use of broad, emotionally charged terms like "cyber attack" creates huge problems. Public officials, business leaders, news media, and private citizens may overreact to events like the 2014 hack of Sony Pictures, which harmed the company, but not national security. Or, they may be so overwhelmed by vulnerabilities and risks that they cannot think strategically. In a 2015 House hearing on global cyber threats, National Security Agency Director Admiral Rodgers warned, *"Terminology and lexicon is very important in this space… I'll hear people throw out attack, act of war, [when] that's not necessarily … how I would characterize the activity that I see."*[5]

Government regulations and analyses by cybersecurity experts provide various ways to categorize malign cyber activity, but none of these categorization schemes is simple yet comprehensive enough to be widely accepted and broadly useful. For example, the FISMA reporting requirements use a taxonomy under which any type of unauthorized access must be reported within one hour of detection, while any attack that disrupted normal operations must be reported within two hours, even though it is not clear why all unauthorized access requires more urgent action than any disruptive attacks do. Malicious code, improper usage, and scans/probes/ attempted access must be reported on a daily, weekly, or monthly basis. In short, respondents are required to report what happened, but not why it happened, what if any impact it had, how severe the effects were, and what recovery required.

New federal incident reporting requirements that took effect on April 1, 2017 ask for more information.[6] Instead of using PPD-41's 5-point scale, respondents must rank functional and informational effects on a seven-point, color-coded scale, ranging from 0/white (negligible effects) to 7/black (emergency)—e.g. an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons. They are also asked whether the recovery time was predictable (not how long it took) and whether the affected organization needed external help to recover. These are important distinctions, but the response options remain subjective and the method works only for post-hoc incident reporting.

For preventive risk assessment and mitigation, organizations can choose among a variety of frameworks, each with their own terminology and methodology. Established risk frameworks, such as Octave, FAIR, ISO 27005, and the National Institute of Standards and Technology (NIST) Risk Management Frameworks focus on risks to individual IT components, looking at the vulnerability of misconfigured and unpatched computers, the likelihood of attack, and the potential impact on specific IT systems. But organizational leaders, policymakers, and other senior-level professionals trying to think strategically about cybersecurity need a risk assessment framework that can help them understand risks and response options more holistically, and

[4] Cichonski et al, 2012, "Computer Security Incident Handling Guide", NIST SP-800-61, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[5] House of Representatives Session titled "Cyber Security Threats", September 2015, https://www.c-span.org/video/?328021-1/hearing-worldwide-cybersecurity-threats

[6] https://www.us-cert.gov/government-users/reporting-requirements.

communicate with each other more productively about how different kinds of cyber events at different types of organizations could affect not only the core missions of that organization, but also public health and well-being, different levels of the economy, critical infrastructure, and homeland or international security.

The CISSM Cybersecurity Framework

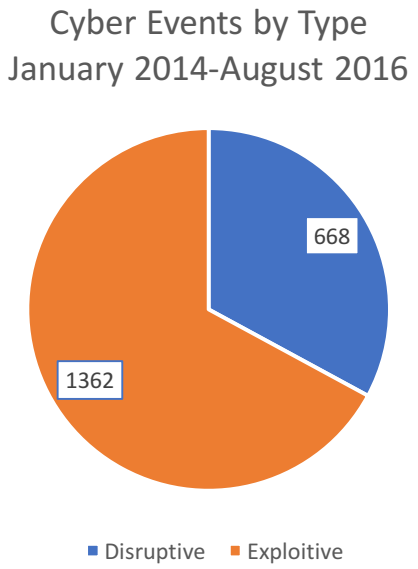
CISSM's approach to categorizing cyber events, evaluating consequences, and prioritizing risks starts by differentiating between two classes of malign cyber activities—cyber exploitation and cyber disruption—based on underlying motivation. It can be difficult to determine the underlying motive for network intrusions that are discovered before any damage has been done, since intruders may use similar tools and techniques to gain access for either purpose. Instead of trying to classify all cyber *incidents*, we only categorize cyber *events*, meaning that observable cyber actions have had harmful consequences for the organization, and possibly also for some larger collective of which that organization is a part (e.g. a business supply chain, the local economy, or some part of a city, state, or country's critical infrastructure).

When the clearest motivation seems to be compromising information for financial gain, political benefit, or national security advantage, we use the term "cyber exploitation." This includes theft of customer records, organizational information, or intellectual property, and can occur in various ways. When the primary objective is to interfere with an organization's operations or the functioning of the larger collective, we term it "cyber disruption."

Cyber exploitation has historically been much more common than cyber disruption, but the frequency and severity of disruptive attacks has increased in recent years. There is no reliable, comprehensive, publicly available dataset of cyberattacks that can be used to determine precisely how the relative frequency of these two classes of malign cyber events are changing over time. To get a rough sense of the frequency of different types of cyber events, CISSM researchers compiled a dataset of 2,030 cyber events from January 2014 through August 2016 that could be identified by systematic web searches, events referenced by blogs, security vendor portals, or other English-language news sources. We only included events for which we could find a direct news source that was verifiable and provided some insight into the methods of the attack.[7] This dataset is not an exhaustive accounting of all cyber events during this time period, nor is it a representative sample. The true population of malign cyber activity is unknown because some significant events are kept secret and many other cyber incidents are too trivial to warrant media attention. Nevertheless, this dataset includes a large enough number of events for it to be useful for illustrating CISSM's categorization and measurement methodology.

One third of the events in the dataset (668) caused some form of disruption, while two-thirds were classified as exploitative. The database includes many different types of events, such as website defacement, compromise of Point of Sale (PoS) machines, large-scale theft from databases, Distributed Denial of Service (DDoS) attacks, and damage to physical control systems. The targets were also diverse, including: educational institutions, government agencies, energy firms, industrial manufacturers, and famous individuals.

[7] The CISSM Cyber events dataset can be provided upon request.



Differentiating among Different Types of Disruptive Cyber Events

Because the ultimate effects of exploitative and disruptive attacks are dissimilar, CISSM has developed two different indices for estimating or measuring their consequences. The remainder of this brief focuses on disruptive cyber events, with CISSM's approach to categorizing and assessing exploitative events described elsewhere.

Disruptive cyber events seek to impact an organization's ability to produce and deliver a good or service in one or more of five ways:

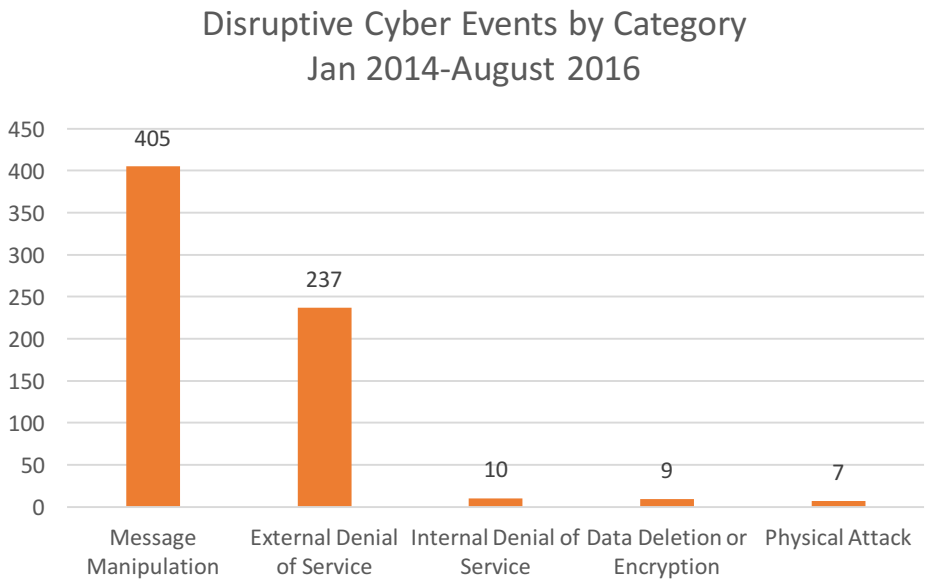
- Message Manipulation: Disruption of an organization's social media presence or website through the hijacking of a user's account credentials or through system vulnerability;
- External Service Disruption: Disruption of external operations through a denial of service (e.g. DDoS);
- Internal Communication Interference: Disruption of operations through interference with network services used for internal communication;
- Data Attack: Disruption of internal operations through multi-point deletion or encryption of user data; and
- Equipment Attack: Disruption of internal operations by physically destroying, manipulating, or disabling equipment control capabilities.

Representative Examples of Cyber Events in Each Category	
Message Manipulation	Turkish hackers replaced the homepage of a Russian Bank with messages boasting about the shooting down of a Russian jet over the Turkey-Syrian border.[8]
External Service Disruption	Two South African organizations had their websites overwhelmed with traffic by DDoS attacks conducted in response to alleged anti-white policies espoused by the groups.[9]
Internal Communication Interference	A Newport Beach, California, cybersecurity firm was the victim of hackers who accessed and reset a core router. That created a cascading failure across the entire internal network, making most of the firm's IT systems unavailable.[10]
Data Attack	The Lansing Board of Water and Light had its e-mail system and internal network rendered inoperable due to the propagation of a ransomware attack.[11]
Equipment Attack	A Ukrainian power company experienced several different cyber events, including the disconnection of breakers thereby denying power to thousands of customers.[12]

Of the 668 disruptive events in our dataset, the vast majority (96%) involve message manipulation or external denial of service. Hackers leveraged easily exploitable vulnerabilities to deface websites, hijack social media accounts by compromising user credentials, or use external computers to flood the victim's outward facing servers with connection requests in order to deny services to legitimate visitors to that organization's website.

Only 26 events (4%) can be categorized as internal communication interference, data attack, or equipment attack. The rarity of these types of events can be attributed to the relative ease that other types of events, such as website defacements and DDOS attacks, can be executed from outside the target network and can be scripted to attack large swaths of internet space.

[8] https://www.hackread.com/turkish-hackers-deface-russian-bank-website/
[9] http://news.softpedia.com/news/anonymous-attacks-anti-white-movements-in-south-africa-and-zimbabwe-505251.shtml
[10] http://arstechnica.com/security/2016/03/after-an-easy-breach-hackers-leave-tips-when-running-a-security-company/
[11] http://news.softpedia.com/news/water-and-lighting-utility-faces-issues-because-of-ransomware-infection-503568.shtml
[12] http://www.theregister.co.uk/2015/12/29/kiev_power_outages_blamed_on_russian_hackers/



Assessing the Severity of Disruptive Attacks on Specific Organizations

Disruptive cyber events can have more or less severe *primary* effects on an organization's operations depending on its mission, its ability to rapidly detect and diagnose the problem(s), and the types of redundancy or recovery measures available to reduce or minimize disruption. For example, some large government agencies and private businesses routinely respond to hackers trying to interfere with web traffic to their servers so quickly that customers hardly notice any delay, while a small company or non-profit may lack the resources to prevent disruption to an important part of their operations. Disruptive cyber events can also have more or less severe *secondary* effects on the users of that organization's services, the larger economy, or the environment, and important consideration for policymakers, but categorizing or measuring these effects is beyond the scope of this paper.

To identify these primary effects clearly, we need to move beyond the categories and scales currently dictated by federal regulations to develop a methodology that many different types of stakeholders can use to evaluate cyber risks, set priorities for protection, share information, and decide when the government needs to get involved in some type of coordinated response. Thinking about how PPD-41's severity schema would apply to the Sony hack, one can easily see how some public officials or company executives might minimize its likely impact on anything other than the company's own finances and reputation, calling it a level 1 (green) event. Others might see it as a level 3 (orange) event because they consider the cyber attacks and subsequent threats against theaters which showed Sony's unflattering film about North Korea's leader as an assault on free speech with a demonstrable impact on civil liberties. The hack even had the potential to meet the criteria for a level 4 (red) event, if it had resulted in U.S. military retaliation and a North Korean response with significant impact on national security and foreign relations.

PPD-41's effort to match observed actions and intended consequences to severity levels is also misleading because the same actions could have very different consequences for different types

of organizations. Moreover, similar cyber events with comparable consequences for internal operations of two different organizations could be a major public concern in one instance, and inconsequential in another. For example, damaging computer and networking hardware is high on PPD-41's severity scale, but could cause only a brief disruption to operations if the affected organization had replacements readily available, and could seem completely inconsequential to government officials if the affected organization was a youth soccer league rather than an electrical utility.

The CISSM framework includes a Cyber Disruption Index (CDI) that can help affected organizations and government officials have a standard way of assessing the consequences of different types of cyberattacks on different types of organizations so they are more likely to agree about when government involvement is warranted. It compares the consequences of an actual or potential cyber event along three dimensions: scope, magnitude of effect on impacted devices, and duration of the disruption. For mathematical reasons, the value assigned on each dimension needs to be greater than zero and no more than one, so that scores on the three dimensions can be multiplied to get a total CDI value that provides a systematic, if still somewhat subjective, way to compare the overall consequences of different types of attacks against different kinds of organizations. These values can be measured after an event. They can also be roughly estimated for different types of potential attacks by analysts with general knowledge. And they can be calculated more precisely by those who have detailed information about how a particular organization's IT networks and procedures map onto its mission and operations.

CDI = Scope x Magnitude x Duration

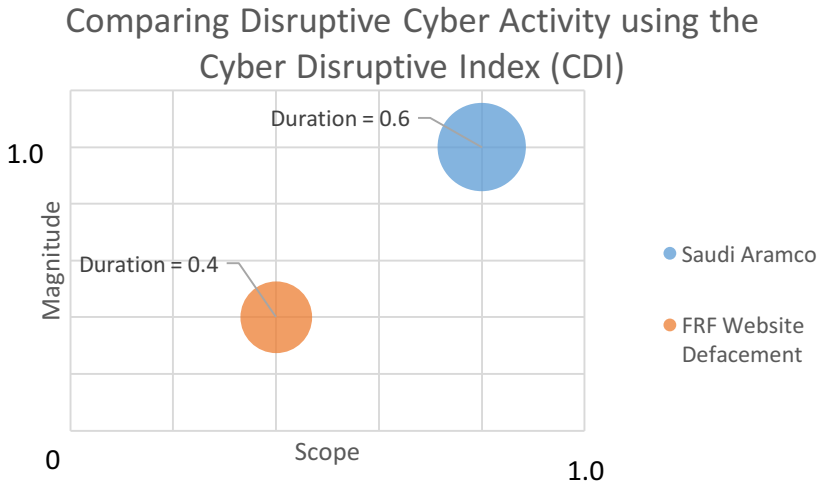
Scope of the Event	Magnitude of the Event	Duration of the Event
Insignificant number and/or importance of devices (0.2)	Insignificant effect on the productivity of equipment (0.2)	Insignificant (minutes) system down time (0.2)
Minimal number and/or importance of devices (0.4)	Minimal effect on the productivity of equipment (0.4)	Minimal (minutes to hours) system down time (0.4)
Significant number and/or importance of devices (0.6)	Significant effect on the productivity of equipment (0.6)	Significant (hours to days) system down time (0.6)
Massive number and/or importance of devices (0.8)	Massive effect on the productivity of equipment (0.8)	Massive (days to weeks) system down time (0.8)
All devices in a network (1.0)	Complete loss of productivity (1.0)	Total (weeks to indefinite) system down time (1.0)

We can illustrate a simplified version of this assessment method using the basic information given in news reports about a high-profile data deletion attack on Saudi Aramco in 2012.[13] The IT networks used for production and distribution were not impacted by the attack, but a massive number of computers (35,000) in the administrative sections of the organization's network were non-functional for more than 24 hours.

With this information, we can assign each dimension a score that ranges from .2 to 1. Someone with more detailed knowledge of the event's consequences could adjust our scores on one or more dimensions, leading to a different CDI value. Because the two CDI values could be broken down into their constituent parts, each with a specific explanation, the reasons for the divergent assessments would be much clearer with CISSM's CDI than with PDD-41's severity scale.

We scored the scope of the Saudi Aramco event as a 0.8 given the massive number of administrative computers impacted, and despite the production and distribution networks not being affected. We scored its magnitude as a 1 given the complete loss of productive value (deletion of hard drives) for every computer hit in the attack. Finally, most systems took over 24 hours to reconstitute, so we scored the duration as 0.6. Taking the product of all three dimensions, the event CDI value was 0.48.

This assessment method can also make explicit why some cyber attacks are implicitly considered to be more or less severe than others, even when different types of attacks and different kinds of organizations are involved. For example, in June 2016, Albanian hackers defaced the Romanian Football Federation (FRF) website after Romania lost to the Albanian national team.[14] We scored the scope of the attack as .4 because the defaced website is a single node of the FRF's IT infrastructure, albeit a relatively important one for this type of fan-based organization. The webserver could still function even though the website was defaced, so we scored the magnitude a .4. The FRF IT department was able to restore the website in a few hours, so we scored the duration as a .4, too. Taking the product of all three dimensions gives a CDI value of 0.06, clearly much less serious than the Saudi Aramco event even if it compounded Romania's humiliating loss on the soccer field.



[13] http://money.cnn.com/2015/08/5/technology/aramco-hack/
[14] http://news.softpedia.com/news/after-football-albania-humiliates-romania-in-cyberspace-as-well-505506.shtml

The CDI can also be used to assess the relative severity of events within the same category of cyber attacks. To do this, we used data from a 2014 report by Kaspersky Labs that included results from a survey of its customers about the impact of DDoS events from April 2013 to May 2014.[15] Roughly 18% of the 3,900 large, medium, and small companies that responded to the survey had experienced a DDoS event, representing an increase in the frequency and total number of DDoS events over previous years.

DDoS events are categorized as *External Service Disruption* events in the CISSM framework. Since all DDoS events target specific internet-facing devices, we scored each event's scope as a .4, because the webserver plays a single, albeit relatively important function in most organizations.[16] The Kaspersky survey provides enough information about the magnitude and duration of each DDoS event for us to differentiate between those that were simply a nuisance versus those that represent a more systemic threat to the organizations' operations. It does not identify the type or name of the affected organizations, information that would be required to assess how serious the second-order effects of a severe DDoS attack could be.

Of the 702 respondents who reported a DDoS attack, only 334 reported effects lasting more than a few seconds. The table below includes only the 334 events that would have had a demonstrable effect on a user experience.

		Magnitude		
		Slight Page Viewing Delays (Score of 0.2)	Significant Page Viewing Delays (Score of 0.6)	Transaction Failures or Complete Disruption (Score of 1.0)
Duration	Less than 10 minutes to an hour (Score of 0.2)	96	14	4
	Several Hours (Score of 0.6)	77	24	5
	Full Day to Several Weeks (Score of 1.0)	89	20	5
Scope is fixed as .4 for all DDoS events because they impact only a single, albeit important, node in the targeted network (e.g. web server).				

The vast majority of these DDoS events involved page viewing delays that stretched from a few minutes to several weeks. While inconvenient for customers and a challenge for internal IT staffs to tackle, page viewing delays rarely meet the standard of a significant cyber incident identified in PPD-41. However, a few incidents do appear to result in complete transactional failures or

[15] "Global IT Security Risks Survey 2014-Distributed Denial of Service (DDoS) Attacks" https://press.kaspersky.com/files/2014/11/B2B-International-2014-Survey-DDoS-Summary-Report.pdf?_ga=1.258421002.1038056443.1457609677

[16] For a broader discussion of scope please see page 6 of "A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact," CISSM Working Paper, July 2015.

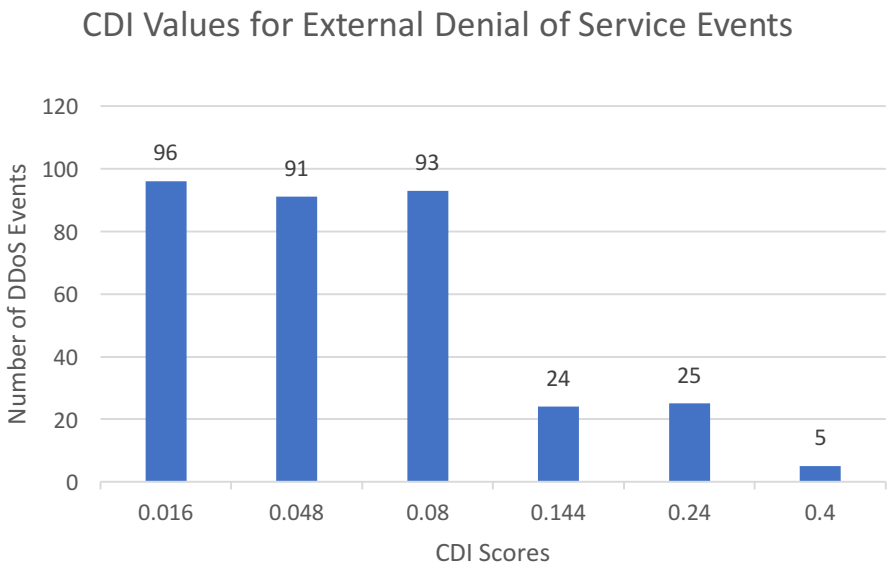
disruption periods of several hours to weeks, likely resulting in significant material losses for the affected organizations.

Calculating the CDI for each event yields a range of scores from 0.016 to 0.4 on a 0 to 1 point scale. For the 334 DDoS events that lasted more than a few seconds, 54 received a CDI score of 0.144 or greater, denoting significant page viewing delays (or worse) lasting at least a few hours.

Only 5 events, less than 1% of all DDoS events reported, caused complete transactional failures or disruptions for more than a day. They still only received a CDI score of 0.4, though, because DDoS attacks have a narrow scope that does not affect internal networks. The organization could still conduct all operations that did not involve externally facing web services unless the DDoS event was part of a campaign that included other types of disruptive attacks on that organization. This differentiates DDoS attacks from other types of disruptive events (e.g. Ransomware attacks on internal networks) that can disrupt internal operations for significant periods of time.

Of the 5 most serious events, a review of the second order effects would help determine which, if any, required government assistance and policy makers' attention. For example, a sustained DDoS against a major U.S. bank, such as the attacks against JP Morgan Chase, could reduce public confidence in a vital sector of the U.S. economy.[17] A comparable DDoS against a small manufacturing company, while highly disruptive for the firm, would not pose serious problems for the economy or the country as a whole.

The chart below displays the breakdown of DDoS incidents reported in the Kaspersky survey by their CDI score.



Implications for Policymakers

PPD-41 is an improvement in the federal government's response to cyber-attacks. It defines the idea of a significant cyber event, appoints an inter-agency group to coordinate a federal government response, and attempts to differentiate between events' levels of severity. But PPD-41 does not go far enough to differentiate among different types of cyber events or to provide a

[17] http://www.scmagazine.com/ddos-attack-strikes-jpmorgan-chase-website/article/284261/

standard methodology for measuring effects on multiple dimensions and comparing the severity of different kinds of attacks on different types of organizations. Nor is it clear how the PPD-41 severity scale could be used by organizational leaders and policymakers to think systematically about plausible future attacks; set priorities; allocate resources for prevention, detection, response, and recovery; and make other strategic risk management decisions

The PPD-41 schema acknowledges that cyber attacks can have more or less severe consequences, but implicitly ranks some categories of events as more serious than others (e.g. destruction of equipment control systems ranks higher than denial of services to external customers even though a long-duration DDoS attack on an important organization that cannot function without reliable website access could have greater economic effects than destruction of one control system at a small company that can quickly switch to a back-up system).[18] Scope and duration are important components of severity but users are not told how they should be included in PPD-41's scale. The lack of a repeatable method of assessing the severity of attacks in the directive makes it difficult to measure the effects of cyber incidents and highlight those that merit greater review by policy makers.

The CISSM framework can be used to help address these problems. By differentiating between disruptive and exploitative events, and among different categories of disruptive and exploitative events, it provides a simple taxonomy that facilitates clear communication between organizations and government about the types of attacks that have occurred. It also encourages organizational leaders and policymakers to think more systematically about the full range of plausible future attacks that could affect their organizations, rather than trying to protect against only the most common tactics.

The three-dimensional CDI provides much needed perspective about how many of the thousands, millions, or even billions of so-called "cyber-attacks" reported by the media actually involve more than a trivial disruption to organizational operations.[19] The vast majority of cyber events in the dataset CISSM compiled from news sources and the one compiled by Kaspersky from customer surveys were not severe enough to warrant any type of coordinated government response.

Using the CISSM framework to think more systematically about what could happen in the future suggests many plausible scenarios in which a cyber attack on some part of the critical infrastructure would be a major public concern, and therefore warrants government attention to risk mitigation as well as incident response. Failure to invest in appropriate risk mitigation measures could lead to human deaths, not just economic damage, if a hospital loses access to patients' electronic medical records in a ransomware attack, or if the equipment control systems of a nuclear power plant or hydro-electric dam were targeted. Electricity or transportation systems for major cities could be shut-down for days, not only by attacks on control systems, but also by other disruptive attacks that public officials may not have even considered. A widespread service disruption lasting hours or days would be bad enough during normal times, but substantially more serious if the city was hosting a global event like the Olympics. Even a sustained DDoS attack against a major bank could be a public policy problem if customers lost confidence in the reliability of the banking system.

[18] https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf
[19] http://www.cybersecurity-insiders.com/cyber-attacks-on-japans-critical-infrastructure-touches-128-billion-mark/222

In short, applying consistent means of categorizing and measuring the effects of disruptive cyber activity will help organizational leaders make better decisions about how much they should invest in what type of cybersecurity risk mitigation measures so they can avoid needing government help responding to a severe attack. It will allow government officials and law makers to have a more nuanced and productive conversation about the types of threats that a country needs to be concerned about, enabling prioritization of resources to maximize the defense, redundancy, or resiliency of critical infrastructure or significant economic players.

About the authors

Charles Harry is vice president for cyber and analytic solutions at Orbis Operations, and a Research Scholar at the Center for International and Security Studies at Maryland. Prior to his work at Orbis, Harry worked for the Department of Defense for 12 years where he led organizations tackling some of the hardest national security challenges. Harry holds degrees in Economics and History from the University of Colorado and a PhD in Policy Studies from the University of Maryland.

Nancy Gallagher is the Director of the Center for International and Security Studies at Maryland (CISSM) and a Research Professor at the University of Maryland's School of Public Policy. Before coming to the University of Maryland, Gallagher worked at the State Department and the Arms Control and Disarmament Agency. She was the Executive Director of the Clinton administration's Comprehensive Test Ban Treaty Task Force. Gallagher is the author of numerous books, monographs, and articles, including *The Politics of Verification*, *Controlling Dangerous Pathogens*, *Reconsidering the Rules for Space Security*, and *Comprehensive Nuclear Accounting*.