VOLUME 3 ◆ NUMBER 1 SPRING 2018

THE CYBER DEFENSE REVIEW

Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum
Major General Patricia Frost
Captain Clifton McClung
Lieutenant Colonel Christopher Walls

Preparing for Cyber Incidents with Physical Effects
Chief Joseph W. Pfeifer

An Airman's View of Deterrence and Cyberspace
General Jay Raymond

Smart Bases, Smart Decisions — *Dr. Harold J. Arata III, Mr. Brian L. Hale*

There IS No Cyber Defense — *Mr. Bryson Bort*

Strategic Blind-Spots on Cyber Threats, Vectors, and Campaigns — *Dr. Cathy Downes*

Countering the Cyber Threat — *Mr. Shawn Henry, Dr. Aaron F. Brantly*

The Role of Commercial End-to-End Secure Mobile Voice in Cyberspace — *Mr. Elad Yoran, Dr. Edward Amoroso*

ARMY CYBER INSTITUTE ◆ WEST POINT

Preparing for Cyber Incidents with Physical Effects

Joseph W. Pfeifer

ABSTRACT

Cyber weapons have been used to steal billions of dollars of intellectual property, influence elections, manipulate news and damage critical infrastructure. Yet, we think of cyberattacks as only a technology problem, which are handled by smart computer network technicians capable of discovering a breach and developing patches to mitigate the problem. Certainly, technical solutions are a big part of cyber preparedness. But what if cyberattacks combine denial of services in cyberspace with targeted attacks on critical infrastructure, causing massive damage and loss of life in the physical world?

This article will explore how federal, state, and local agencies, as well as private corporations, are using tabletop exercises, functional simulations and war gaming to prepare for significant cyberattacks. These programs examine how public and private sectors adapt to extreme cyber events. In a connected world, adaptive incident managers quickly form networks to exchange ideas, align core efforts and foster public communication.

Designing Cyber Exercise

Today's threat environment of state-actors, terrorists, criminals, and hackers could use cyberattacks to causes physical harm as a substitute for kinetic assaults. This dramatic shift from guns and bombs changes how we perceive risk and preparedness. Cyber exercises need to identify gaps in prevention, protection, mitigation, response and recovery procedures. However, well-designed exercises also create the conditions to develop new skills and partnerships for managing the impact of a cyber event. Examining the experience of exercise participants is not only about observing behavior, but also is about understanding cognitive processes when overwhelmed by mass destruction that has not been fully imagined. Exercises, simulations and war games

Joseph Pfeifer is the Chief of Counterterrorism and Emergency Preparedness for the New York City Fire Department (FDNY). During his career, he has commanded responses to some of the largest disasters in New York City's history. He was the first Chief at the World Trade Center attack on September 11, 2001, played a major command role during Hurricane Sandy in 2012, and helped manage NYC's Ebola Response. He is the founding director of FDNY's Center for Terrorism and Disaster Preparedness, a senior fellow at the Combating Terrorism Center at West Point, and a senior fellow at the Program on Crisis Leadership at the Harvard Kennedy School. Pfeifer has spoken at United Nations Conferences and the World Knowledge Forum, and testified to the U.S. Congress about the threats cities will face in future. He holds Master's Degrees from the Harvard Kennedy School, Naval Postgraduate School, and Immaculate Conception and has written widely in professional journals.

are ways to gain insight into decision-making when under stress and confronted with novelty.

Over the past year, three noteworthy cyber exercises were conducted to build a framework for mitigation and response to multi-sector cyberattacks on major cities. The first was by the Army Cyber Institute (ACI) in cooperation with New York City agencies (FDNY, NYPD, NYCEM, DOITT, DEP) and Citigroup. The ACI designed an exercise that combined a functional computer keyboard operator piece requiring technicians to defend the network against a "live-fire" from an opposing "red team" in a virtual environment, along with a tabletop exercise for senior leaders from the emergency response community, water supply, utilities, banking, telecommunication, health, and transportation. This two-day exercise was useful because it promoted interactions between technicians and emergency response leaders. [1]

The second exercise was a simulation conducted by FDNY's *Center for Terrorism and Disaster Preparedness (CTDP)* for cadets from the United States Military Academy at West Point. Cadets enrolled in Homeland Security and Cyber classes were brought to the FDNY's Operation Center in Brooklyn to participate in a realistic simulation. These cadets formed an Incident Management Team (IMT) that managed state and local responders who worked with military assets during a cyber incident with physical effects on New York City. They then had to report their operational plan to FDNY's Chief Counterterrorism and The New York Adjutant General of the National Guard who were part of the exercise. Utilizing an IMT to handle the consequences of a cyberattack with physical damage proved invaluable to coordinating a multi-sector response. [2] The IMT shared information across sectors and coordinated federal, state and local operations.

The third exercise was a series of cyberwar games designed by Naval War College (NWC) against private sector critical infrastructure. With 85% of all critical infrastructure owned by the private sector, senior leaders from 15 critical infrastructure sectors, including financial services, food and agriculture, chemical, energy, dams, wastewater, defense industry, healthcare, and communication, committed two full days to war gaming.[3] These industries engaged with Department of Defense (DoD), federal, state and local officials in war games that simulated targeted attacks by nation and non-state actors on U.S. critical infrastructure. The task was to manage the cyber and physical events as senior leaders kept government officials, infrastructure owners and the public informed.[4]

While each of these exercises had a slightly different focus, they all shared a common scenario of a major cyberattack on critical infrastructure in a densely-populated city. Events included distributed-denial-of-services (DDoS) attacks on the financial sector, hospital medical information ransomware demands, and physical destruction by manipulating Program Logic Controllers (PLC) and Supervised Control and Data Acquisition (SCADA) systems. The effect of the cyberattacks released hazardous radiation and chemicals, contaminated water and food supplies, crippled parts of the electrical power grid and communication systems, denied 911 telephone services (TDoS), and triggered air, rail, and road transportation accidents.

The exercise designers arranged a series of cyberattacks to create cascading effects across sectors. As systems become more interdependent, cross-sector cyberattacks increase the risk of catastrophic consequences. This is especially concerning when there are few cross-sector ties for information-sharing and crisis management during cyber with physical damage.

Sharing Information and Situational Awareness

As the cyber exercises unfolded, operators of critical infrastructure and emergency responders were absorbed by events that appeared to look almost routine. The financial sector questioned why their ATMs were not working, as emergency responders were called to multiple emergencies. Each sector, influenced by organizational bias, became so preoccupied with solving their own problem that they became oblivious to what was occurring outside their group.[5] But with the spread of service outages and an uptick of emergencies, there was a need for greater situational awareness regarding the entire event.

Situational awareness is a threefold process of perception, comprehension, and anticipation.[6] During a significant cyberattack, this search for situational awareness becomes more complicated as senior leaders and organization fail to recognize the signs that events are taking place across both the cyber and physical domains. This is further obscured by not understanding the interdependency of these two worlds and the inability to anticipate what could happen next.

All three exercises illustrate the struggle to fully comprehend the connections between a cyberattack and the resulting physical events. Failure to acquire multiple levels of situational awareness limits one's ability to manage and mitigate the incident. Organizations turn into themselves and focus only on their presenting problems. Even when organizations wanted to grasp the bigger picture, there was a lack of knowing how to share information and who to collaborate with across sectors.

The *National Cyber Incident Response Plan,* based on *Presidential Preparedness Directive 41,* attempts to address this gap in information sharing and coordination.[7] It calls for the private sector to report cyber incidents to their Information Sharing Analysis Center (ISAC), arranged by particular sectors, e.g., financial, chemical, energy, etc. The plan also talks about the FBI sharing information with the intelligence community. Influenced by organizational bias, these well-intended procedures can create *stovepipe situational awareness,* where information is only shared within a particular sector.

Connecting diverse groups of people during a cyber-attack to share information at the physical incident and away from the incident in a computer center is the challenge. In most exercises, participants make these connections notionally. However, the ability to connect through voice, video, and data is critical for information sharing. Cyber exercises have identified the lack of knowing how and who to connect at the federal, state and local levels as a significant gap in preparedness. Organizations and sectors need to be able to push and pull information not only about their part of the incident, but also about the global effects of the incident.

As part of an improvement plan, we must explore how to map out network ties for information sharing during cyber events. Constructing a network map would visually display what agencies need to connect to each other for situational awareness. This could be tasked to Department of Homeland Security (DHS) Fusion Centers, whose main function is to share information for homeland security. These state and urban area Fusion Centers do not command or control resources; instead, they should become the conduit for moving information so others in government and the private sector can better exchange ideas and align core efforts. Fusion Centers form information hubs, which decentralize the flow for more timely and accurate reporting.

Managing the Incident

The next preparedness advancement in cybersecurity is to develop the skills to manage an incident in the dual world of cyber with physical effects. While malware can be planted in systems long before an attack takes place, a significant cyberattack with physical effects will most likely take place quickly to shock and avoid adaptive response. The initial shock and cumulative stress of an evolving incident could cause a loss of system control, stovepipe situational awareness, ineffective coordination, and a drop in public confidence for government to mitigate the damage.

As a cyber incident begins, technicians start to connect to each other to mitigate the attack on their systems. If these attacks have physical effects, first responders will form teams of firefighters, police officers, and EMTs/paramedics to jointly respond to the emergencies. At the same time, federal, state and the local Emergency Operations Center and the National Cybersecurity and Communications Integration Center will start to connect to each other to build a comprehensive operating and resource assessment picture. The National Guard and federal resources will also begin to mobilize assets to mitigate the incident. How these groups form vary greatly depending on if they emerge from the federal, state or local levels. Connecting these groups requires the creation of hastily constructed communication networks. [8]

A network structure emerges when parts of the public and private sectors begin to connect and coordinate with each other. The same evolutionary process occurs for crisis management during other catastrophic events such as natural disasters, terrorist attacks, large-scale accidents, and major wildland fires. At the early stages of an incident, random networks appear, then emerge into a more organized cluster pattern, and finally when an incident is nearly stabilized a more centralized hub-type network begins to form. Response to extreme cyber events is a process of emergence that starts with a convergence of public and private sector response groups that self-organize into a more connected network. From little order emerges a complex social system of clusters. Each central node shares information within and outside its cluster, which begins to create a network system of incident management.

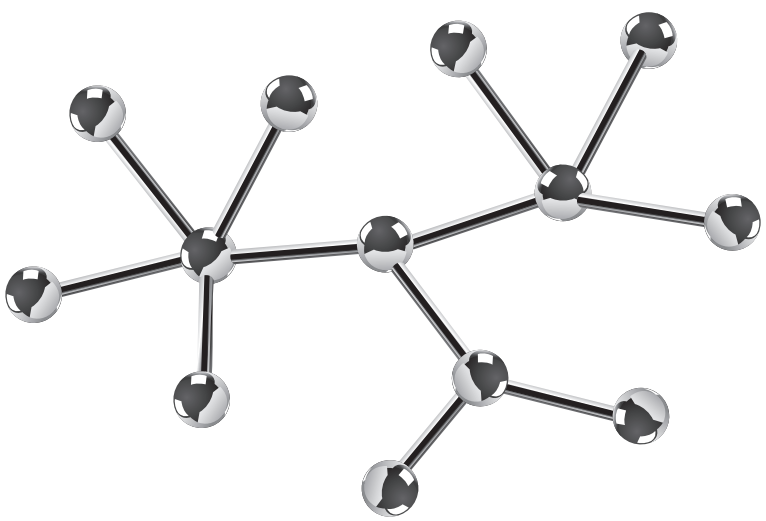

Figure 1. Networks connect public and private sectors for information sharing, response coordination and public messaging.

Crisis leadership is about forming clusters and getting clusters to communicate and coordinate with each other. The *National Response Plan* (NRP), *National Incident Management System* (NIMS) and *National Cyber Incident Response Plan* provide a framework for incident management. NIMS, in particular, can play a significant role in shaping the physical and cyber management space, yet this is rarely used in cyber exercises. The problem is that incident management is viewed as a hierarchical, top-down structure, when in reality incident management emerges from the bottom up. During a significant cyber incident, there are many different response organizations separated by geography and function. The incident management system guides the building of a management structure that includes elements of command, operations, planning, logistics, and administration. As the incident grows, clusters form area commands, which connect to other clusters (hubs) for information and resources. The actual shape of the response network is dependent on the ties between clusters.

IMT's trained for a cyber incident with physical effects can play an essential part in shaping the cyber incident response network. These teams are different than the Computer Emergency Response Team (CERT) whose function is to mitigate computer security incidents on the network side. A Cyber-IMT, similar to the West Point cadet simulation, bridges the gap between the cyber and physical world by connecting technical cyber mitigation with different parts of the response network for information sharing and incident management. Building these teams with the trained personnel will take a considerable amount of effort, which could be tasked to each FEMA region. Such efforts are beginning to be discussed by DHS and others in the private sector. In the energy sector, they are exploring the idea of "Cyber Consultants." These Cyber-IMTs could be incorporated nicely into the *National Cyber Incident Response Plans.*

Communicating with the Public

Since every significant cyber incident is political, the third component of cyber preparedness is the ability to communicate with the public and government officials. This involves public messaging, press briefings, countering fake news, and holding conference calls with officials from the federal, state, and local government. All three exercises tested public communications. One simulation used video cameras and microphones with tough reporters to simulate a real press briefing. The spokesperson must be knowledgeable about what is occurring, empathetic to the people affected by the incident, and explain what is being done to manage the incident. Complicating public messaging is fake news, which could be misinformation and part of the cyberattack or simply rumor. In any case, frequent updates to the public are useful countermeasures.

Public officials have a responsibility to effectively manage information and the incident. Therefore conference calls with Secretaries, Governors, Mayors, and other officials are extremely important. At times, it may be beneficial to include the CEO of critical

infrastructure as part of this call. These conference calls need to be held at least once a day. This political communication engagement is a critical element of cyber exercises that should be tested with at least senior leaders' staffers.

Preparing for the Future

Cyber preparedness leverages exercises, simulations, and war games to strengthen a response network for information sharing, incident management, and public communication. This network model of public and private sectors is flexible enough to adapt and respond to cyber incidents with physical effects. The challenge is to pinpoint the connections or ties that shape the network of cyber and emergency response partners. These connections bridge gaps between the cyber and physical world for exchanging critical information and coordinating response efforts. Even a small number of bridging ties can dramatically accelerate the spread of information within a system.[9] Senior leaders are dependent on timely information for situational awareness so they can make decisions that shape a response network to mitigate the effects of cyberattacks.

General (Ret.) Stanley McChrystal argues that robustness is achieved by strengthening parts of the system, while resilience is the results of linking elements that allow resources to be reconfigured or adapted to a changing environment.[10] He refers to this as *Team of Teams* working on different parts of a mission. In our attack scenario, it requires multiple teams to manage the incident in the virtual and physical world.

Cybersecurity is about strengthening prevention efforts and mitigating attacks in this domain. Cyber preparedness is not only about cybersecurity, but it is also about coordinating a response in the physical world. This will take teams of people from both the public and private sectors. The challenge to maintain homeland security and business continuity is to understand how to reconfigure the network of teams to leverage each other to manage both the cyber and physical dimensions of an attack.

NOTES

1. Army Cyber Institute, *After Action Review,* (West Point), 2016. This Cyber exercise, named Jack Voltaic, is the first in a series of ACI multi-sector cyber and dual function (mitigation/response) exercises with major cities.

2. FDNY, *After Action Review,* (New York), 2017.

3. J. Schneider, *Cyber Attacks on Critical Infrastructure,* Insight from War Gaming, https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming, 2017.

4. Naval War College, *War Gaming Exercise Plan.* (Newport, RI), 2017.

5. Joseph Pfeifer, "Crisis Leadership: The Art of Adapting to Extreme Events." *Harvard Kennedy School's Program on Crisis Leadership Discussion Paper Series,* (Cambridge, MA: Harvard Kennedy School: 2013), 5.

6. Mica Endsley, *Toward a theory of situation awareness in dynamic systems,* Human Factors [H.W. Wilson - AST], Mar 1995, Vol. 37, 32.

7. DHS, *National Cyber Incident Response Plan,* (Washington, D.C., 2016).

8. P.J. Denning, Hastily formed networks. *Communication of the ACM, 49*(4), 2006, 15-20.

9. David Lazer and Maria Christina Binz-Scharf, "It Takes a Network to Build a Network" in *Governance and Information Technology: From Electronic Government to Information Government,* edited by Viktor Mayer-Schonberger and David Lazer, (Cambridge: The MIT Pres, 2007), 266.

10. Stanley McChrystal with Tantum Collins, David Silverman, and Chris Fussel, *Team of Teams: New Rules of Engagement for a Complex World,* (New York: Portfolio/Penguin, 2015), 80.