UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 18 | Issue 2 Article 3

12-1-2016

Is Cyberattack the Next Pearl Harbor?

Lawrence J. Trautman

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 18, ISSUE 2: DECEMBER 2016

IS CYBERATTACK THE NEXT PEARL HARBOR?

Lawrence J. Trautman*

Central Intelligence Agency Director, Leon Panetta, states in his Secretary of Defense confirmation testimony before the Senate Armed Services Committee that, "[t]he next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems."[1] *Cyberattacks have become a daily threat to businesses, consumers,*

---

* BA, The American University; MBA, The George Washington University; post-graduate studies (Management Information Systems) University of Texas at Dallas; and JD, Oklahoma City University School of Law. Mr. Trautman is Assistant Professor of Business Law and Ethics, Western Carolina University, a past president of the Dallas Internet Society and the New York and Metropolitan Washington/Baltimore Chapters of the National Association of Corporate Directors. He may be reached at Lawrence.J.Trautman@gmail.com. The author wishes to express particular thanks to Professor Julie J.C.H. Ryan for the inspiration provided by the students of her Information Operations EMSE6537 class in the School of Engineering and Applied Sciences, Engineering Management and System Engineering Department at The George Washington University. My thanks also to those who reviewed all or parts of this manuscript and provided candid and constructive critiques: Braden Allenby; Steven Anderson; Chris Bronk; Anupam Chander; Jamie Gorelick (9/11 Commission); Sherri Harte; Gen. Michael V. Hayden; Sarah Jane Hughes; Mitchell Kominsky; Joanna Kulesza; John Norton Moore; Julie J.C.H. Ryan; Peter Swire; and Tim Trautman. Particular thanks to Admiral Bobby R. Inman, USN (Retired), Former Director of the National Security Agency and Deputy Director of Central Intelligence; Congressman Lee H. Hamilton; Vice Chairman, 9/11 Commission, Former Chairman, House Committee on Foreign Affairs and Former Chairman, U.S. House Permanent Select Committee on Intelligence; and Congressman Michael McCaul, Chairman of the U.S. House Homeland Security Committee.

[1] Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack,* THE CHRISTIAN SCIENCE MONITOR (June 9, 2011), http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.

and all nation states resulting in the profound loss of economic assets and intellectual property. Cyberattack represents a real threat to geopolitical stability and world peace. This article depicts a fictional scenario of what a cyberattack on a massive scale might look like and examines current and historical factors to better understand how such a devastating cyberattack is set in motion and how we might avoid it.

IS CYBERATTACK THE NEXT PEARL HARBOR?

"Attacks against us are increasing in frequency, scale, sophistication and severity of impact. Although we must be prepared for a catastrophic, large-scale strike, a so-called 'Cyber Armageddon,' the reality is that we've been living with a constant and expanding barrage of cyber attacks for some time."

Hon. James R. Clapper
Director of National Intelligence
February 26, 2015 [2]

I. OVERVIEW

Central Intelligence Agency Director, Leon Panetta, stated in his Secretary of Defense confirmation testimony before the Senate Armed Services Committee that, "the next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems."[3] Cyberattacks have become a daily threat to businesses, consumers, and all nation states, resulting in the profound loss of economic assets and intellectual property. Cyberattack represents a real threat to geopolitical stability and world peace.[4]

---

[2] James Clapper, *Opening Statement of Worldwide Threat Assessment Hearing Senate Armed Services Committee* (2015), http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee (last visited Mar. 25, 2016) (statement made by Hon. James R. Clapper, Director of National Intelligence).

[3] Anna Mulrine, *supra* note 1.

[4] *See generally* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,* 25 HARV. J.L. & TECH. 429 (2012); Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?,* 25 STAN. L. & POL'Y REV. 269 (2014); Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Proctor, Aileen Elizabeth Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEX. L. REV. 1533 (2010); *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology:Hearing Before the H. Subcomm. on Oversight and Investigations, Comm. on Foreign Affairs,* 112th Cong. 112-14 (2011); Nathan Alexander Sales, *Regulating Cyber-Security,* 107 NW. U.L. REV. 1503 (2013);

This article depicts a fictional scenario of what a cyberattack on a massive scale might look like. First, is a possible scenario of such a cyberattack. Second, for historical perspective, the December 7, 1941 attack on Pearl Harbor is presented. Third is a review of contemporary and credible warnings. Fourth is a discussion about the privacy versus national security debate, and geopolitical developments that might determine how a cyber drama is played-out on the world stage. Fifth, the question of what is to be done is addressed. Next, the 1946 Congressional Joint Committee on the Investigation of the Pearl Harbor Attack's recommended principles (designed to prevent the repetition of such a future attack) is reviewed with our contemporary environment in mind.

II. ZERO DAY

"And ye shall know the truth and the truth shall make you free."

John 8:32 (King James)[5]

Scott Shackelford & Amanda Craig, *Beyond The New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity,* 50 STAN. J. INT'L L. 119 (2014); Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage,* 46 CONN. L. REV. 1165 (2014); Peter Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?,* 2 J. TELECOMM. & HIGH TECH. L. (2004); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE J. INT'L L. 421 (2011); Paul Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons,* YALE L. & POL'Y REV. (forthcoming), http://ssrn.com/abstract=2364658; Kristen Eichensehr, *The Cyber-Law of Nations,* 103 GEO. L.J. 317 (2015); Peter Sommer & Ian Brown, *Reducing Systemic Cybersecurity Risk (*Org. for Econ. Cooperation and Dev., Working Paper No. IFP/WKP/FGS(2011)3), 2011) http://ssrn.com/abstract=1743384; William Banks, Developing Norms for Cyber Conflict (2016) (unpublished paper), http://ssrn.com/abstract=2736456 (depicting 1982 massive explosion of the trans-Siberian pipeline caused by malware apparently inserted into Canadian software).

[5] *John* 8:32 (King James).

Zero Day

What happened? It's a Tuesday morning in February. Without fanfare or warning, Americans awake to find that nothing works. In Wellesley, Massachusetts, sixth graders at Horatio H. Hunnewell Elementary School on Cameron Street awoke later than usual because alarm clocks failed to provide their normal wake-up call. Meanwhile, just a few miles away in South Boston, the fire fighters of Engine Company 39, Ladder 18 receive delayed notice of homes ablaze because the phone system is down. First responders arrive at their destinations later than normal because traffic lights are not functioning. Everywhere this morning, fire fighters are busy dealing with fires, hamstrung because fire hydrants are not operational due to electrical outages that cause pumps to fail. Those individuals reliant on electrical medical devices are struggling, and confusion is widespread.

This Tuesday morning, the electrical grids in the eastern and western United States fail.[6] As a result, all states except for Texas, Alaska and Hawaii (which have their own grids) are without power. The government declares a state of emergency and promises to locate the problem and restore services as soon as possible. Emergency generators provide power for some essential services such as hospitals and public broadcasters. However, schools are closed, and public transportation proves intermittent at best. Inoperable traffic signals cause automobile travel to slow to a snail's pace in major cities. Phone landlines are down for most businesses. Cell towers don't work because of power loss. Some people use this "holiday" from work and school to venture out for necessities. However, stocked groceries and operating gas stations prove hard to come by since few sources have their own power generators. Most restaurants are unable to open due to lack of electricity and public transportation for their employees. With memories of 9/11 and the use of air transportation for purposes of

[6] *See generally* TED KOPPEL, LIGHTS OUT: A CYBERATTACK; A NATION UNPREPARED; SURVIVING THE AFTERMATH (Crown Pub., 2015) (depicting a future attack on U.S. power grids and its aftermath). *See also* Richard J. Kisielowski, *Hey America! Let's Get Smart: The Need for a Reliable Modern Smart Electrical Grid Resistance to Cyberattacks,* 24 CATH. U. J.L. & TECH. 139 (2015).

terrorism still too fresh,[7] immediate orders are given for all air traffic to land at the nearest possible airport. All originating air travel is cancelled, resulting in the stranding of travelers numbering in the tens of thousands, usually at unfamiliar airports. Even so, just before all aircraft could land, reports of compromised aircraft control systems are reported. Also, within recent memory are the terrorist attacks at Fort Hood,[8] the Boston Marathon,[9] Paris,[10] San Bernardino,[11] and Brussels.[12]

---

[7] *See generally* Derek Jinks, *September 11 and the Laws of War*, 28 YALE J. INT'L L. (2003), http://ssrn.com/abstract=391640; Michael A. Hitt, Katalin Takacs Haynes & Roy Serpa, *Strategic Leadership for the 21st Century*, 53 BUSINESS HORIZONS 437 (2010), http://ssrn.com/abstract=1995786 (observing that "the attacks on the World Trade Center in New York and the Pentagon in Washington produced a significant loss of lives, and changed the political and business landscapes for many decades to come"); Jason Bram, James Orr & Carol Rapaport, *Measuring the Effects of the September 11 Attack on New York City*, 8 FRBNY ECON. POL'Y REV. (Nov. 2002), http://ssrn.com/abstract=802786; Garrick Blalock, Vrinda Kadiyali & Daniel H. Simon, *The Impact of 9/11 on Road Fatalities: The Other Lives Lost to Terrorism,* 41 APPLIED ECON. (2005), http://ssrn.com/abstract=677549 (finding that following the terrorist attacks of Sept. 11, 2001, driving fatalities increased significantly as travelers used autos rather than air, and then this effect weakened over time as drivers returned to air transportation); John Yoo & Robert J. Delahunty, *The President's Constitutional Authority to Conduct Military Operations Against Terrorist Organizations and the Nations that Harbor or Support Them,* 25 HARV. J. L. & PUB. POL'Y (2002), http://ssrn.com/abstract=331202.

[8] *See generally* Tung Yin, *Were Timothy Mcveigh and the Unabomber the Only White Terrorists?: Race, Religion, and the Perception of Terrorism*, 4 ALA. C.R. & C.L. L. REV. 33 (2013), http://ssrn.com/abstract=2049221.

[9] *See generally* Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U.L. REV. 21 (2013), http://ssrn.com/abstract=2373527; Matt Saldaña, *Counterterrorism Roadblocks: Constitutional Under the Fourth Amendment?,* 40 OHIO N.U.L. REV. 585 (2014), http://ssrn.com/abstract=2424314; Alexander J. Blenkinsopp, Note*, A Different Perspective on the Boston Lockdown,* 48 NEW ENG. L. REV. 1 (2013), http://ssrn.com/abstract=2271595; Joanna Wright, *Applying Miranda's Public Safety Exception to Dzhokhar Tsarnaev: Restricting Criminal Procedure Rights by Expanding Judicial Exceptions,* 113 COLUM. L. REV. SIDEBAR 136 (2013), http://ssrn.com/abstract=2333989; Dawinder S. Sidhu, *Lessons on Terrorism and 'Mistaken Identity' from Oak Creek, with a Coda on the Boston Marathon Bombing,* 113 COLUM. L. REV. SIDEBAR 76 (2013), http://ssrn.com/abstract=2263565; W. Kip Viscusi & Richard J.

California

The Urth Café on Melrose is famously the breakfast hub and meeting spot of working Hollywood and movie industry executives. But this morning, no spinach & feta omelets are served. Like Florida, southern Texas and Arizona, the West Coast—particularly southern California—benefits from a climate that is hospitable even during February. At the macro level, widespread losses of electrical power result in store closures and quicker defrost and spoilage of existing grocery store foodstuffs. The inability to pump gas at most service stations quickly results in long lines of cars waiting to fuel at the few open gas stations (before resupply trucks fail to make deliveries). Abandoned cars left on streets and highways soon become a major problem for the already congested Los Angeles area.

In northern California, Sandhill Road in Menlo Park, just a few minutes from Stanford University, is "ground zero" for America's venture capital industry. This morning, many pillars of venture finance find themselves locked out of their offices when front door electronic security devices fail to operate. Classes are cancelled at Stanford, and lunch will not be served today along Fisherman's Wharf in San Francisco.

Even during February, the impact of global warming and wildfires prove to be problematic this year in the western United States. Lack of transportation hinders both first responder emergency services, such as firefighting efforts, and the ability to move agricultural products to heavily populated areas. Widespread

---

Zeckhauser, *Recollection Bias and Its Underpinnings: Lessons from Terrorism-Risk Assessments* (Harvard Kennedy Sch., Working Paper No. 16-003) (2015), http://ssrn.com/abstract=2692253.

[10] *See* Adam Nossiter, Aurelien Breeden & Katrin Bennhold, *Paris Attack Was the Work of Three Teams, An 'Act of War' By ISIS, France Asserts*, N.Y. TIMES, Nov. 15, 2015, at A1; *see also* Andrew Higgins & Milan Schreuer, *'They Did Not Give Anybody a Chance',* N.Y. TIMES, Nov. 15, 2015, at A1.

[11] *See* Devlin Barrett, Saeed Shah & Tamara Audi, *Focus Turns to Wife's Role in Assault,* WALL ST. J., Dec. 7, 2015, at A6; Damian Paletta, Siobhan Hughes & Jim Carlton, *Shooters Were 'Radicalized,'* WALL ST. J., Dec. 8, 2015, at A1.

[12] *See* Natalia Drozdiak, Gabriele Steinhauser & Matthias Verbergt, *Terror Strikes Europe's Heart,* WALL ST. J., Mar. 23, 2016, at A1.

hunger soon becomes the primary cause of civil unrest and crime. Frightened people quickly resort to desperate measures.

For California, as in most of the United States, most component parts of the electrical grid are now many decades old. Critically important for transferring electrical power between circuits, large power transformers average forty years old, with many in operation for an excess of seventy years.[13] After power failures from disasters such as Hurricane Sandy on the U.S. east coast, the grid's "reliability, effectiveness, and affordability are increasingly being brought into question."[14] However, not enough was done to fix the grid.

National Capital Area

This morning, breakfast is not available at the Hay Adams Hotel across from the White House. Nor were the doors open for business at Busboys and Poets at 2021 14th Street, NW.[15] All the typical tourist attractions like the Smithsonian Museums remain closed, along with public schools. Classes are cancelled at American, Catholic, Georgetown, George Washington, Howard, and the University of the District of Columbia.

The bureaucratic army of the Potomac is estimated to employ over 500,000 federal workers, not counting the thousands of lawyers and consultants that perform work primarily for the U.S. government.[16] Almost all remain at home this day. As any thoughtful cyber warfare strategist might have predicted, an attack on the metropolitan Washington, DC – Baltimore metroplex is a focal point of the hostilities. Primary targets were the cyber warriors located at the suburban Washington, DC headquarters of

---

[13] Brian Warshay, *Upgrading the Grid: How to Modernize America's Electrical Infrastructure,* FOREIGN AFF., Mar.–Apr. 2015, at 125.

[14] *Id.*

[15] BUSBOYS AND POETS, http://www.busboysandpoets.com/ (last visited Nov. 17, 2016).

[16] *See Federal Employees By State*, GOVERNING.COM, http://www.governing.com/gov-data/federal-employees-workforce-numbers-by-state.html (reporting data on the concentration of federal employees compiled from 2013 Bureau of Labor Statistics Current Employment Statistics).

the National Security Agency (NSA),[17] the Northern Virginia defense community represented by the Central Intelligence Agency (CIA),[18] and the almost 30,000 employees who work at the Pentagon.[19] In addition to these well-known agencies are the many whom the press seldom acknowledges as they engage in the mission of defending the United States against attacks both physical and virtual.

Day Three: Internet Backbone and Fiber Cable Destroyed

Because most had not enjoyed Internet availability since Zero Day due to lack of power, the sabotage and loss of the undersea international fiber cable system a few days after the initial attack on the U.S. power grid remained generally unnoticed. This submarine fiber optic network is "the physical infrastructure that underpins the virtual cloud of cyberspace."[20] Since its advent in 1977, the fiber optic cable system has experienced rampant growth. Thomas Friedman observes, "around the year 2000 we entered a whole new era, Globalization 3.0 . . . . [which brings] the newfound power for *individuals* to collaborate and compete globally."[21] Friedman contends this development allows rapid circulation of digital content at almost no cost, thus creating global collaboration. Therefore, "[g]lobalization 3.0 is going to be more and more driven not only by individuals but also by a much more diverse—non-western, non white—group of individuals. Individuals from every corner of the flat world are being empowered."[22]

---

[17] *Contact Us*, NATIONAL SECURITY AGENCY, https://www.nsa.gov/about/contact-us/ (last visited Nov. 17, 2016).

[18] *Contact CIA*, CENTRAL INTELLIGENCE AGENCY, https://www.cia.gov/index.html# (last visited Nov. 17, 2016).

[19] Barbara Maranzani, 9 *Things You May Not Know About the Pentagon*, HISTORY.COM (Jan. 15, 2013), http://www.history.com/news/9-things-you-may-not-know-about-the-pentagon.

[20] Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis,* 24 CATH. U. J. L. & TECH. 57, 58 (2015).

[21] THOMAS L. FRIEDMAN, THE WORLD IS FLAT 3.0: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY, 10 (Picador 2007).

[22] *Id.* at 11.

To put the loss of oceanic submarine cable communication infrastructure into perspective, consider that during 2010, the United Nations recognized "submarine communications cables as 'critical communications infrastructure' and 'vitally important to the global economy and the national security of all States.'"[23] Davenport continues to warn that "submarine fiber optic cables provide the vast majority of international telecommunications—some 95% overall."[24] As the Internet's backbone, submarine cables carry over $10 trillion daily in transactions for over 8,300 financial institutions on the SWIFT (Society for Worldwide Interbank Financial Transactions) network.[25]

Boston—Days, Then Weeks Later

It is nine degrees in suburban Boston, and for most residents there has been no heat for several weeks. Almost overnight, money has no meaning; bartering replaces currency for transactions, and the American economy grinds to a halt. Banks are closed, and ATM machines fail to operate.

Down on Wall Street, although emergency backup systems are capable of trading securities, orders to buy or sell are not received in New York, as Boston area brokerage offices lack telephone service and have no ability to communicate. Commerce ceases nationwide as the power grid continues to stay down. Backup systems powered by fossil fuels soon deplete their supplies of coal, gas, diesel, kerosene, *et cetera*. Much like the great blizzard of 2015, snow is piled up everywhere.[26] Schools have not reopened since Zero Day. Public transportation remains closed. After several days, snow removal is finally abandoned for lack of fuel and because workers choose to be at home with their families.

---

[23] Davenport, *supra* note 20, at 62 (citing G.A. Res. 65/37, ¶ 121 (Dec. 7, 2010)).

[24] Davenport, *supra* note 20, at 62 (citing LIONEL CARTER ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD 8 (2009), http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf).

[25] Davenport, *supra* note 20, at 63.

[26] Alex Sosnowski, *How Did East Coast Blizzard of 2015 Play Out?*, ACCUWEATHER (Jan. 31, 2015), http://www.accuweather.com/en/weather-news/what-happened-to-the-forecast/41294989.

Ambulance, fire, and police services quickly become missing in action. But this time, things are different.

It's been almost ten days now since electricity went out across forty-seven states. For a while, hospitals are okay with their backup power sources. Within a week or so, many start to run out of fuel to power their generators. At first, elective surgeries are postponed. Several days later as power becomes increasingly scarce, medical monitoring machines fail and lab testing stops. Doctors, nurses, and other healthcare workers cannot make their way between home and work. By now, most hospitals are desperately understaffed, without fuel or other sources of functioning power. Many hospitals simply fail and services stop, with no place to send their patients. The sick start to die and bodies pile up. Without electricity, gas stations cannot pump gas, streetlights and traffic signals are dark, and those who can make it through the snow soon empty grocery stores of all remaining usable food.

At sub-freezing temperatures, humans and their habitats are in peril. As buildings shed their heat, staying warm becomes a challenge. The elderly and the very young succumb first. After the first few days, finding fire for warmth becomes difficult and causes panic. After firewood supplies are consumed, all things paper, and even fine furniture, are burned for warmth. Staying warm in large cities proves particularly challenging. The silent killer of carbon monoxide poisoning leads to accidental deaths.[27]

When elevators fail to work, having navigated many flights of stairs in the dark to get home, many of those living in apartment buildings stay inside. It takes days for emergency workers to rescue those caught in stalled elevators when the power failed. Fire becomes an unchecked inferno, as desperate city dwellers create fires from anything that will burn. In the absence of vital emergency services, these fires inevitably become uncontrollable. First buildings, then entire neighborhoods, burn out of control.

---

[27] April Kahn, *What Is Carbon Monoxide Poisoning?*, HEALTHLINE (Dec. 1 2015), http://www.healthline.com/health/carbon-monoxide-poisoning#Overview1.

With transportation halted, after a week or so hunger forces many to go into the cold in search of something to eat.

The Midwest in February

The weather in Chicago is almost always horrible in February.[28] This year is no different. Many resourceful residents in Evanston and the more affluent suburbs use their gas fireplaces for cooking. However, this proves to be much easier to do in theory than in practice. Before long, cooking grease results in fires and dangerous and painful burns. Similar human misery is found throughout the mid-west as cities like Detroit, Cleveland, Columbus and St. Louis quickly stall to a frozen halt.

In the South

Those in warmer climates find survival moderately easier. In rural areas, crops and livestock provide sustenance. Many revert to those survival skills typical of life on the prairie two hundred years earlier. Even worse than the gas lines of the 1970s, service station fuel pumps fail for lack of electrical power, and transportation soon stops as cars are rendered useless due to lack of fuel. Railroad and truck food distribution systems in the South also fail, and the population soon grows hungry. Hunting and fishing moves from being a hobby to a necessity, and survival gains a renewed importance in daily life. Particularly in densely populated areas, household pets soon disappear, along with the residents of many local zoos. Animal shelters everywhere are no longer needed. Easy availability of firearms results in a rapid shift of vital resources between the "haves" and "have nots."

As the homeless have known for years, survival in warmer climates, such as in Florida, is easier during the winter. Unlike the frozen northeast, it is actually possible to sleep outdoors during the winter. As a result, many families in the northern parts of the United States, having abandoned all their belongings, once their

[28] Christian Farr, *Record-Breaking Cold Air Grips Chicago*, NBC CHICAGO 5 (Feb. 19, 2015), http://www.nbcchicago.com/weather/stories/chicago-weather-record-cold-thursday-february-18-292218691.html.

gas runs out now find themselves stranded in their cars somewhere between home and their southern destinations.

The Importance of Water

As those in the western part of the United States have known for years, water scarcity is a life or death issue. Messrs. Papa, Casper, and Moore state that "[s]upervisory control and data acquisition (SCADA) systems and industrial control systems (ICSs) are widely used to control systems such as water supply systems, wastewater collection and treatment facilities. . . . Unfortunately, . . . these systems are vulnerable to command injection[29] and middle-person attacks."[30]

James Fugate, now Administrator of the U.S. Federal Emergency Management Agency (FEMA),[31] developed his emergency management skills while serving as Florida's State Coordinating Officer[32] during eleven federal disasters,[33] including the four major hurricanes impacting Florida in 2004,[34] and three more in 2005.[35] Fugate observes, "[w]e're not a country that can

---

[29] *See* Stephen Papa, William Casper & Tyler Moore, *Securing Wastewater Collection Systems from Accidental and Intentional Harm: A Cost-Benefit Analysis,* 6 INT'L. J. CRITICAL INFRASTRUCTURE PROTECTION 96-97 (2013) (*citing* W. Gao, T. Morris, B. Reaves & D. Richey, *On SCADA Control System Command and Response Injection and Intrusion Detection,* IEEE ECRIME RESEARCHERS SUMMIT (ECRIME), 1 (Oct. 2010)).

[30] *Id.* at 97 (*citing* Stephen Papa, William Casper & S. Nair, *A Transfer Function based Intrusion Detection System for SCADA Systems,* IEEE INT'L CONF. ON TECH. FOR HOMELAND SEC. 93 (Nov. 2012)).

[31] FEDERAL EMERGENCY MANAGEMENT AGENCY, https://www.fema.gov/ (last visited Nov. 17, 2016).

[32] *Emergency Coordinating Officer Information*, FLORIDA DIVISION OF EMERGENCY MGMT., http://www.floridadisaster.org/eco/index.asp (explaining the role of State Coordinating Officer).

[33] *See William Craig Fugate*, FEMA: LEADERSHIP (July 15, 2016), https://www.fema.gov/william-craig-fugate.

[34] *2004 Hurricane Season: Five Years Later*, FLORIDA DIV. OF EMERGENCY MGMT. (Aug. 11, 2011), http://floridadisaster.org/hurricanes/2004/.

[35] *See generally* Post Disaster Development Planning (2006), http://www.floridadisaster.org/recovery/documents/Post%20Disaster%20Redevelopment%20Planning%20Guidebook%20Lo.pdf.

go without power for a long period of time without loss of life. Our systems, from water treatment to hospitals to traffic control to all [those] things that we expect every day, our ability to operate without electricity is minimal."[36] The availability of water is a major priority at all times, particularly during a disruptive crisis such as a cyberattack. According to Fugate,

> That means we need to have enough power to pump, treat, and distribute water through the system. You have to keep the water system up, and you've gotta [sic] then focus on the water treatment system. Backing up sewage is just about as bad. Those two pieces will buy you enough time to look at what your alternatives are. Basically, people have to drink water, they have to eat, that waste has to go somewhere, they need medical care, they need a safe environment. There has to be order of law there.[37]

The nation's water supply presents numerous vulnerabilities. The control system of a small dam within twenty miles of New York City was reported to have been hacked by Iranian hackers in 2013.[38] The DOJ unsealed an indictment during March 2016 charging a defendant who was working on behalf of the Iranian Government to hack into the supervisory control and data acquisition systems of the Rye, New York Bowman Dam, thereby providing the ability to control flow rates and water levels.[39]

---

[36] *See* KOPPEL, *supra* note 6, at 117.

[37] *See id.* at 118.

[38] *See* Danny Yadron, *Iranian Hacking Threat Emerges,* WALL ST. J., Dec. 21, 2015, at A1. *See also* Robert M. Lee, *Takeaways from Reports on Iranian Activity Against the Power Grid and a Dam,* SANS INDUSTRIAL CONTROL SYSTEMS SECURITY BLOG (Dec. 21, 2015), https://ics.sans.org/blog/2015/12/21/takeaways-from-reports-on-iranian-activity-against-the-power-grid-and-a-dam (suggesting elements of the *Wall Street Journal* article are misleading and that defenders must get smarter and keep the opportunity to damage infrastructure out of the hands of malicious actors); *see also* Dustin Volz & Nate Raymond, *U.S. to Blame Iran for Cyber Attack on Small NY Dam: Sources,* REUTERS: TECHNOLOGY NEWS (Mar. 10, 2016), http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WC2NH; Rebecca Smith, *Utilities Work on Strategy to Stem Blackouts,* WALL ST. J., Apr. 8, 2016, at B1.

[39] *See* Press Release, Loretta E. Lynch, Attorney General, U.S. Department of Justice, Attorney General Loretta E. Lynch Delivers Remarks at Press

Constituting a threat to public health and safety, The *Wall Street Journal* reports that, "America's power grid, factories, pipelines, bridges and dams−all prime targets for digital armies−are sitting largely unprotected on the Internet . . . [since] [m]any of the computers controlling industrial systems are old and predate the consumer Internet. [All] 57,000 industrial-control systems, . . . more than any other country,"[40] remain vulnerable targets.

Communication Systems

When the national electrical grids fail, home routers, televisions, most elements of the Internet of Things ("IoT"),[41] and landline telephones become useless. After the relatively few commercial and home generators run out of their fuel sources, batteries for personal computers, iPads, iPhones, and all other hand-held devices soon lack connectivity and the ability to gain battery recharge. While public broadcasting facilities tend to have backup generators, cable television likely does not operate in most homes due to the lack of household electrical power. Car radios soon become the largest source of news and widespread civil-defense-type communication, until the gasoline runs out.

International Impact

France and Great Britain also experience attacks similar to those aimed at the United States. Somehow, German technology

---

Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-press-conference-announcing-seven.

[40] *See* Yadron, *supra* note 38, at A1, A16.

[41] *See infra* note 163; *see also* Neil Gershenfeld & JP Vasseur, *As Objects Go Online: The Promise (and Pitfalls)of the Internet of Things,* FOREIGN AFF. Mar.–Apr. 2014, at 60; Anupam Chander, Robots, the Internet of Things, and the Future of Trade, UC Davis Legal Studies Research Paper No. 465 (2015), http://ssrn.com/abstract=2679028; Derek Harp, *The Rise of The Things!,* SANS INDUSTRIAL CONTROL SYSTEMS BLOG (Oct. 12, 2015), *https://ics.sans.org/blog/2015/10/12/the-rise-of-things* (last viewed Apr. 13, 2016); Derek Harp, *The Rise of the Things #2,* SANS INDUSTRIAL CONTROL SYSTEMS BLOG (Nov. 12, 2015), https://ics.sans.org/blog/2015/11/12/the-rise-of-the-things-2.

prevailed, and actual damage to the German strategic infrastructure was modest. Global financial markets shut down in New York, London and Paris. As a result, the values of financial instruments everywhere are in free fall (based on the few remaining open markets). As you might expect, just like with the United States-inducted financial meltdown of 2008,[42] global counter-party transaction risk results in worldwide economic contagion.[43] The global historical engines of economic growth—sales of automobiles[44] and homes[45]—immediately grind to a halt, along

---

[42] *See generally* Robert C. Hockett, *Six Years on and Still Counting: Sifting Through the Mortgage Mess,* 9 HASTINGS BUS. L. J. 1 (2013), http://ssrn.com/abstract=2029262 (describing complex nature of causal factors of mortgage crisis resulting in lengthy healing process); GARY B. GORTON, SLAPPED IN THE FACE BY THE INVISIBLE HAND: BANKING AND THE PANIC OF 2007 (2009), http://ssrn.com/abstract=1401882; Gary B. Gorton & Andrew Metrick, *Securitized Banking and the Run on Repo* (Yale International Center for Finance, Working Paper No. 09-14, 2010), http://ssrn.com/abstract=1440752; Michael D. Hurd & Susann Rohwedder, *Effects of the Financial Crisis and Great Recession on American Household 1s (*Netspar Discussion Paper No. 09/2010-046, 2010), http://ssrn.com/abstract=1708074; Lawrence J. Trautman, Personal Ethics and the U.S. Financial Collapse of 2007-08 (unpublished article) http://ssrn.com/abstract=2502124.

[43] *See generally* Nicole M. Boyson et al., *Hedge Fund Contagion and Liquidity Shocks*, 55 J. FIN. 1789 (2010), http://ssrn.com/abstract=884202; GEERT BEKAERT ET AL., GLOBAL CRISES AND EQUITY MARKET CONTAGION (2012), http://ssrn.com/abstract=1856881; LISA R. GOLDBERG ET AL. EXTREME RISK MANAGEMENT (2009), http://ssrn.com/abstract=1341363; Franklin Allen & Ana Babus, *Networks in Finance* (Wharton Fin. Inst. Center, Working Paper No. 08-07, 2008), http://ssrn.com/abstract=1094883.

[44] *See generally* Pasquale Schiraldi, *Automobile Replacement: A Dynamic Structural Approach,* 42 RAND J. ECON 2 (2011), http://ssrn.com/abstract=1350034; GERARD P. CACHON & MARCELO OLIVARES, DRIVERS OF FINISHED GOODS INVENTORY PERFORMANCE IN THE U.S. AUTOMOBILE INDUSTRY (2009), http://ssrn.com/abstract=980728; KIM HILL ET AL. CENTER FOR AUTOMOTIVE RESEARCH, CONTRIBUTION OF THE AUTOMOTIVE INDUSTRY TO THE ECONOMIES OF ALL FIFTY STATES AND THE UNITED STATES (2015), http://www.autoalliance.org/files/dmfile/2015-Auto-Industry-Jobs-Report.pdf (reporting that over 7 million private sector U.S. jobs are supported by auto manufacturers, suppliers and dealers, representing annual compensation of $500 billion); Owen Irvine, *Sales Persistence and the Reductions in GDP Volatility* (Fed. Reserve Bank of Boston, Working Paper No. 05-5, 2004), http://ssrn.com/abstract=760267; Valerie A. Ramey & Daniel J. Vine, *Tracking*

with the sale of consumer goods. Perhaps more than any other measures, international financial markets illustrate the extent to which markets have become interdependent, and citizens are all in this together.[46]

Now, to reflect upon and seek insight from an important moment in United States history that occurred over seventy-five years earlier.

III. ATTACK ON PEARL HARBOR: DECEMBER 7, 1941

"The modern American intelligence community traces its roots to Pearl Harbor. Everything since that attack has been designed to prevent strategic surprise. We were surprised on September 11. People wanted to know why."

Gen. Michael V. Hayden

---

the Source of the Decline in GDP Volatility: An Analysis of the Automobile Industry (Fin. and Econ. Discussion Series Paper No. 2005-14, 2005), http://ssrn.com/abstract=724921.

[45] *See generally* Paul Emrath, *Impact of Home Building and Remodeling on the U.S. Economy,* NATIONAL ASSOCIATION OF HOME BUILDERS (May 1, 2014), https://www.nahb.org/en/research/housing-economics/housings-economic-impact/impact-of-home-building-and-remodeling-on-the-u-s--economy.aspx; Home Builders Federation, *Economic Importance of Home Building Dictates Positive Budget* (June 17, 2010), http://www.hbf.co.uk/media-centre/news/view/economic-importance-of-home-building-dictates-positive-budget/.

[46] *See generally* John Beirne & Jana Gieck Bricco, *Interdependence and Contagion in Global Asset Markets*, 22 REV. INT'L ECON. 639 (2014), http://ssrn.com/abstract=2476695; Francis X. Diebold & Kamil Yilmaz, *Measuring Financial Asset Return and Volatility Spillovers, with Application to Global Equity Markets*, 119 ECON. J. 534 (2009), http://ssrn.com/abstract=1313919; Lawrence J. Trautman, *American Entrepreneur in China: Potholes on the Silk Road to Prosperity,* 12 WAKE FOREST J. BUS. & INTELL. PROP. L. 427 (2012), http://www.ssrn.com/abstract=1995076 (describing co-dependency of the U.S. and Chinese economies); Kristin J. Forbes, *The "Big C": Identifying Contagion* (Nat. Bureau of Econ. Research, Working Paper No. w18465, 2012), http://ssrn.com/abstract=2164590; Thijs D. Markwat et al. *Contagion as Domino Effect in Global Stock Markets* (Erasmus Research Inst. Of Mgmt. Report Series Reference No. ERS-2008-071-F&A, 2008),http://ssrn.com/abstract=1303880.

Former Director of the National Security Agency and CIA[47]

At 7:53 a.m. Sunday morning December 7, 1941, the United States Naval base at Pearl Harbor, Hawaii was attacked by the Imperial Japanese Navy.[48] As a result, "[e]ighteen ships of the American Pacific Fleet were sunk or badly damaged, including eight battleships."[49] "One hundred and eighty-eight aircraft were destroyed (mostly on the ground) and 2,403 people were killed."[50] The United States declared war on Japan the next day and entered World War II.[51]

Value of Code-breaking

Of particular relevance to this discussion is the evidence suggesting that better and quicker communication between various elements of the U.S. intelligence apparatus could have saved lives by providing warning of the impending attack. In 1937, building on the work of great American cryptanalysts such as Herbert O. Yardley, Laurance F. Safford, Agnes Meyer Driscoll, William F. Friedman, Frank B. Rowlett, Genevieve Grotjan, and many others, relevant "solutions of intercepted foreign messages began flowing to the White House."[52]

Peter Kross writes that "[i]n 1941, William Friedman had broken the Japanese cryptosystem called Purple, which allowed this country to read all the diplomatic traffic coming from Tokyo to its outposts around the world."[53] David Kahn writes that "[b]y late 1941 solutions . . . soared to 50 to 75 messages a day . . . [and]

---

[47] MICHAEL V. HAYDEN, PLAYING TO THE EDGE 153 (Penguin Books 2016).

[48] SECOND WORLD WAR HISTORY, TIMELINE OF THE JAPANESE ATTACK ON PEARL HARBOR, http://www.secondworldwarhistory.com/attack-on-pearl-harbor.asp (last visited Nov. 17, 2016).

[49] *Id.*

[50] NIGEL WEST, A THREAD OF DECEIT: ESPIONAGE MYTHS OF WORLD WAR II 68 (Random House 1st ed. 1985).

[51] *See id.*

[52] David Kahn, *The Intelligence Failure of Pearl Harbor,* FOREIGN AFF., Winter 1991-1992, at 44.

[53] PETER KROSS, THE ENCYCLOPEDIA OF WORLD WAR II SPIES 268 (Barricade Books, 1st ed. 2001).

a PURPLE message on July 31, 1941 from . . . Tokyo to the ambassador in Washington declared: There is more reason than ever before for us to arm ourselves to the teeth for all-out war."[54] Moreover,

> In the first week of December, 1941, the U.S. learned that the Japanese government gave instructions to its Washington embassy to start destroying its codes, a clear sign that diplomatic relations were about to be broken. On December 6 through 7, U.S. code breakers intercepted a 14-part message, the so-called 'War Warning,' which ended with orders to break off any further talks with the Americans at precisely 1:00 p.m. Washington time (7:30 a.m. Hawaii time) on December 7.[55]

American code-breaker and mathematics teacher Frank Rowlett observes, "As I look back at all the messages and other information available to us . . . it becomes crystal clear to me that this message ordering the destruction of certain of Washington's codes provided the necessary evidence . . . which would make war between the United States and Japan a certainty."[56] Pearl Harbor had not been protected. As Kahn writes, "Japan had sealed all possible leaks. The ambassadors in Washington were not told of the attacks. Knowledge of it was limited in Toyko to as tight a circle as possible . . . No reference to a raid on Pearl Harbor ever went on the air, even coded."[57] In a tragedy of errors, "[d]isorganization and divided responsibility had cost America dearly."[58] It had taken fifteen and a half hours after message No.

---

[54] *See* Kahn, *supra* note 52.

[55] KROSS, *supra* note 53, at 269.; *see also* FRED B. WRIXON, CODES, CIPHERS & OTHER CRYPTIC & CLANDESTINE COMMUNICATION: MAKING AND BREAKING SECRET MESSAGES FROM HIEROGLYPHS TO THE INTERNET (1998) (observing that "[d]espite later criticisms of misjudgment, inaction and poor communication, the U.S. cryptography staffs had done their work as quickly as the methods and governmental limitations of that time permitted.").

[56] MICHAEL SMITH, THE EMPEROR'S CODES: THE BREAKING OF JAPAN'S SECRET CIPHERS 97 (Arcade Publishing, NY, 2001).

[57] *See* Kahn, *supra* note 52, at 44.

[58] *See* JAMES BAMFORD, THE PUZZLE PALACE: INSIDE THE NATIONAL SECURITY AGENCY, AMERICA'S MOST SECRET INTELLIGENCE ORGANIZATION 62 (Penguin Books, 1982).

910 (ordering Japan's Washington embassy to destroy all cipher equipment and codes that remained) was first intercepted (seven hours after the attack began) for it to finally reach "a devastated General Short."[59]

Congressional hearings were held by the Joint Committee on the Investigation of the Pearl Harbor Attack during 1945.[60] Seven prior investigations concerning the Pearl Harbor attack produced "9,754 printed pages of testimony from 318 witnesses and the attendant 469 exhibits."[61] The work of the Joint Committee itself resulted in the taking of some 15,000 pages of testimony "and a total of 183 exhibits received incident to an examination of 43 witnesses."[62] The report asks why "with the almost certain knowledge that war was at hand, with plans that contemplated the precise type of attack that was executed by Japan on the morning of December 7—[w]hy was it possible for Pearl Harbor to occur?"[63]

Lessons from History

The surprise attack on Pearl Harbor is not an event anyone under the age of seventy-five will remember from actual life experiences. Therefore, the knowledge most U.S. citizens have about Pearl Harbor comes from history books and may seem increasingly remote as the years pass. For many families, the oral histories passed down by parents and grandparents are how many contemporary Americans remember and learn about Pearl Harbor. Michael McCaul, Chairman of the House Homeland Security Committee, recalls, "My dad's mission—the mission that millions of other young Americans joined after the attack on Pearl Harbor—was to help roll back the threat posed by a radical

[59] *Id.* at 61.
[60] S. Rep. No. 79-244 at xiv, Investigation of the Pearl Harbor Attack: Report of the Joint Committee on the Investigation of the Pearl Harbor Attack (1946).
[61] *Id.*
[62] *Id.*
[63] *Id.* at 253.

ideology."[64] Thoughtful people everywhere will do well to consider that, "those who cannot remember the past are condemned to repeat it."[65]

During World War II, "the increasing sophistication of the information carrying and processing technologies provided a substrate for the development of new ways of executing strategic operations."[66] Professor Julie Ryan observes that the

> contributions of science and . . . operations research . . . to leverage information in systems and engineering led the way . . . for the role of information. Tactical information victories, such as the information skirmishes that preceded the Battle of Midway, highlighted the increasing interaction of advanced communications technologies with strategic deception tactics for operational advantage."[67] As Professor Chris Bronk observes, "[h]ow states behave with regard to the Internet appears to matter more and more within international affairs . . . [and] Internet conflict may be a new area of international behavior falling somewhere between diplomacy and military action.[68]

While a detailed discussion of the law of cyberwar is beyond the scope of this paper, any threshold inquiry must start with the question, "What exactly constitutes 'warfare?'" According to Nineteenth century military theorist Carl von Clausewitz, an act of war requires that aggressive or defensive conduct be (1) "violent or potentially violent, (2) "instrumental: [where] physical violence or the threat of force is a means to compel the enemy to accept the attacker's will," and (3) "attributable to one side at some point

---

[64] MICHAEL MCCAUL, FAILURES OF IMAGINATION: THE DEADLIEST THREATS TO OUR HOMELAND–AND HOW TO THWART THEM 5 (New York: Crown Forum 2016).

[65] GEORGE SANTAYANA, THE LIFE OF REASON OR THE PHASES OF PROGRESS 284 (Charles Scribner's Sons 1905).

[66] *See* JULIE RYAN, LEADING ISSUES IN INFORMATION WARFARE AND SECURITY RESEARCH vii (ACPI, 2015).

[67] *Id.*

[68] *See* Christopher Bronk, *Blown to Bits: China's War in Cyberspace, August-September 2020,* 5 STRAT. STUD. Q. 1, 3 (2011), http://www.au.af.mil/au/ssq/2011/spring/bronk.pdf.

during a confrontation."[69] As of 2013, "[n]o known cyberattack has met all three of those criteria," observes Thomas Rid, contending that "the hype about everything 'cyber' has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future."[70]

In his critique of Thomas Rid's thesis, Jarno Limnéll contends that by 2014 the world had become so "immersed in technology that activities in cyberspace [had] become inseparable from the every-day operations of business, education, government and the military. Actions online affect actions offline, and vice versa. Thus, far from being separate from conventional war, as Rid [contends], cyberwar is deeply embedded in contemporary military practices."[71] Moreover, "[c]yberwar, in fact, is part of the evolution of conventional warfare, which itself is linked to broader social and political change . . . ."[72]

In addition to causing physical injury or death, violence can refer to mental abuse and different forms of deprivation. The academic discipline of peace studies has for decades advanced the concept of structural violence, such as racism and sexism. In its widest sense, then, violence can be found in almost any coercive situation. And the various attacks and activities associated with cyberwar, from stealing data to disrupting other governments' computer systems, clearly fall within this broad category.[73]

This debate, carried out in the pages of *Foreign Affairs*,[74] includes Thomas Rid's concurrence that cyberspace activities are indeed "an inherent part of conventional warfare . . . [and that] the

---

[69] *See* Thomas Rid, *Cyberwar and Peace,* FOREIGN AFF., Nov. 2013, at 77, 78.

[70] *Id.* at 77; *but see* Ido Kilovaty, *Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter,* 4 J. L. & CYBER WARFARE (2015) (arguing that "Article 2(4) of the UN Charter on the prohibition on the threat or use of force ought to apply to economic cyber-attacks").

[71] *See* Jarno Limnéll & Thomas Rid, *Is Cyberwar Real?: Gauging the Threats,* FOREIGN AFF., Mar.–Apr. 2014, at 166.

[72] *Id.*

[73] *Id.*

[74] *See* Thomas Rid, *supra* note 69 at 77, 78.

psychological impact, not just the physical violence, of cyberattacks matter." However, Rid disagrees with Limnéll's conclusion that "waging cyberwar still remains the business of the armed forces alone."[75]

IV. CONTEMPORARY WARNINGS IGNORED

"Knowing what we know now, there will be no explaining our inaction after the next attack."

Gen. Michael V. Hayden
Former Director of the National Security Agency and CIA[76]

Singer and Friedman believe that "[d]efining cyberwar need not be so complicated. The key elements of war in cyberspace all have their parallels and connections to warfare in other domains . . . war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence."[77] For example, "the US government's position is that to meet this definition of the use of force, a cyberattack would have to 'proximately result in death, injury or significant destruction.' That is, even if conducted through cyber means, the effect must be physical damage or destruction."[78]

House Homeland Security Chairman Michael McCaul reflected on the 9/11 Commission's "lack of readiness;" finding, where

---

[75] *See* Thomas Rid, *Is Cyberwar Real?: Gauging the Threats/Rid Replies,* FOREIGN AFF., Mar.–Apr. 2014, at 167. *See also* Mary L. Dudziak, *Legal History as Foreign Relations History, Explaining the History of American Foreign Relations* (Emory Legal Studies Research Paper No. 14-298, 2014), http://ssrn.com/abstract=2476016 (explaining how law has been used as a tool in international relations); Ben Saul & Kathleen Heath, *Cyber Terrorism, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE (Sydney Law School Research Paper No. 14/11, 2015), http://ssrn.com/abstract=2387206.

[76] *See* HAYDEN, *supra* note 47, at 335.

[77] P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 121 (Oxford University Press 1st ed. 2014).

[78] *Id.*

"[t]he most important failure was one of imagination."[79] For those age thirty-five or younger, it may be hard to recognize that widespread availability of the Internet dates back only to the 1990s in the United States. For many other countries, infrastructure development would subsequently lead to increased usage rates as shown in "Exhibit One" below.

Exhibit One[80]

World Internet Usage and Population Statistics

WORLD INTERNET USAGE AND POPULATION STATISTICS
JUNE 30, 2016 - Update

World Regions	Population (2016 Est.)	Population % of World	Internet Users 30 June 2016	Penetration (% Population)	Growth 2000-2016	Users % of Table
Africa	1,185,529,578	16.2 %	339,283,342	28.6 %	7,415.6%	9.4 %
Asia	4,052,652,889	55.2 %	1,792,163,654	44.2 %	1,467.9%	49.6 %
Europe	832,073,224	11.3 %	614,979,903	73.9 %	485.2%	17.0 %
Latin America / Caribbean	626,054,392	8.5 %	384,751,302	61.5 %	2,029.4%	10.7 %
Middle East	246,700,900	3.4 %	132,589,765	53.7 %	3,936.5%	3.7 %
North America	359,492,293	4.9 %	320,067,193	89.0 %	196.1%	8.9 %
Oceania / Australia	37,590,704	0.5 %	27,540,654	73.3 %	261.4%	0.8 %
WORLD TOTAL	7,340,093,980	100.0 %	3,611,375,813	49.2 %	900.4%	100.0 %

NOTES: (1) Internet Usage and World Population Statistics updated as of June 30, 2016. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau, Eurostats and from local census agencies. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, disclaimers, navigation help and methodology, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit and placing a link to www.internetworldstats.com. Copyright © 2001 - 2016, Miniwatts Marketing Group. All rights reserved worldwide.

[79] *See* MCCAUL, *supra* note 64, at 2 (citing THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 155 (2004), http://www.9-11commission.gov/report/911Report.pdf) (observing that Admiral Bobby Inman, a veteran of the intelligence community who served in senior positions at the CIA, DIA, and NSA, said that 9/11 was "grounded in a failure of the Imagination, the kind in which you don't know what you are looking for; you don't know where to look. We didn't see the enemy coming. Because we didn't want to.").

[80] World Internet Usage and Population Statistics, INTERNET WORLD STATS (June 30, 2016), http://www.internetworldstats.com/stats.htm.

As might be expected, discovering Internet capabilities and vulnerabilities proves to be a work in progress. For example,

> In 2007, U.S. soldiers took smartphone photos of a group of new U.S. Army helicopters parked at a base in Iraq and then uploaded them to the Internet. The helicopters weren't classified and the photos showed no seemingly useful information to the enemy. But the soldiers didn't realize the photos also included "geotags," which revealed where the photographers had been standing. Insurgents then used these geotags to pinpoint and destroy four of the helicopters in a mortar attack. Experts now use this example to warn people to be more careful about what they share when engaged in an important activity.[81]

Warnings Abound

Despite the repeated warnings from arguably the best and brightest among us, actual action has proved too little too late. Congress finally passed five major pieces of cybersecurity legislation during December 2014, the first cybersecurity laws enacted in more than a decade.[82] By the time the 2016 U.S. presidential campaign was underway, and following the late 2015 terrorist strikes in Paris, San Bernardino, and Brussels, national security and cyber vulnerability had become topics of major concern to the American public.[83] Dean and law professor Jon M. Garon[84] states, "[t]he effect of these attacks has been to refocus

---

[81] SINGER & FRIEDMAN, *supra* note 77.

[82] *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?,* 2015 U. ILL. J.L. TECH. & POL'Y 341, 341 (2015) (citing Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress,* HARV. NAT'L SEC. J. (Feb. 6, 2014), http://harvardnsj.org/2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress/), http://ssrn.com/abstract=254856.

[83] *See generally* Janet Hook, *New Poll Finds National Security Now Top Concern,* WALL ST. J., Dec. 15, 2015, at A4. *See also* Matt A. Mayer, *It's Too Easy for Terrorists,* WALL ST. J., Dec. 10, 2015, at A15; Greg Ip, *Terror Toll is Beyond Economic,* WALL ST. J., Dec. 3, 2015, at A2.

[84] *Faculty and Staff Profile for* Jon M. Garon, NOVA SOUTHEASTERN UNIV., https://www.law.nova.edu/faculty/administration/garon-jon.html (last visited Oct. 16, 2016).

public and private officials on efforts to reduce the threat of terrorism . . . Perhaps the most tangible effect of this terrorist activity is the momentum it provided to enact the Cybersecurity Act of 2015."[85] Observing that "[t]he omnibus $1.1 trillion spending law also includes hundreds of millions of dollars to add cybersecurity for the IRS, EPA, and other agencies," Dean Garon warns, "[t]he law provides little more than a fig leaf for privacy protection, so only the development of final implementing regulations will determine whether there are meaningful safeguards from the potential abuse of the data sharing provisions to intrude on individual privacy."[86]

General Michael V. Hayden, former director of both the National Security Agency ("NSA") and Central Intelligence Agency ("CIA") warned during 2011 that

> [o]ur most pressing need is clear policy, formed by shared consensus, shaped by informed discussion, and created by a *common* body of knowledge. With no common knowledge, no meaningful discussion, and no consensus . . . the policy vacuum continues. This will not be easy . . . it will require courage; but, it is essential and should itself be the subject of intense discussion.[87]

Commander of U.S. Cyber Command and National Security Agency ("NSA") Admiral Mike Rogers characterized "cyber attacks as the greatest long-term threat to national security in part

---

[85] Jon M. Garon, Dean and Professor of Law, Nova Southeastern University Shepard Broad College of Law, Remarks at the meeting of the 2015 Winter Working Meeting of the American Bar Association, Business Law Section Cyberspace Law Committee meeting (Jan. 30-31, 2015) (citing Public Law No: 114-113, Dec. 18, 2015 (Division N—Cybersecurity Act of 2015)), http://ssrn.com/abstract=2707756.

[86] *Id.* at 5.

[87] *See* Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?,* 2015 U. ILL. J.L. TECH. & POL'Y 341, 343 (2015), http://ssrn.com/abstract=2548561 (citing Gen Michael V. Hayden, *The Future of Things "Cyber,"* STRAT. STUD. Q. 3 (2011)).

because 'we have yet to come to a broad policy and legal consensus.'"[88]

Also during 2011, Deputy Secretary of Defense William Lynn[89] stated, "If we can minimize the impact of attacks on our operations and attribute them quickly and definitively, we may be able to change the decision calculus of an attacker."[90] According to the Pentagon, the volume of intellectual property stolen annually exceeds the amount of information contained in the Library of Congress.[91]

During April 2012, subcommittees of the U.S. House Committee on Homeland Security held hearings on the topic of "Iranian Cyber Threat to the U.S. Homeland."[92] On August 8, 2012, John O. Brennan,[93] at that time Assistant to the President for Homeland Security and Counterterrorism, gave his "U.S. Policy Toward Yemen" speech before the Council on Foreign Relations. Following his prepared remarks, Mr. Brennan stated that the consequence of the failed cybersecurity legislation is that "we're not going to have enhanced authorities and capabilities of the U.S. government to deal with what is an increasingly serious cyber

---

[88] *Id.* at 344 (citing Scott Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity,* N.Y.U. J. LEGIS. & PUB. POL'Y 1, 3 (2014), http://ssrn.com/abstract=2531733).

[89] Press Release from Chuck Grassley, U.S. Senator, Nomination of Mr. William Lynn to Deputy Secretary of Defense (Feb. 11, 2009), http://www.grassley.senate.gov/news/news-releases/nomination-mr-william-lynn-deputy-secretary-defense.

[90] *See* Julian E. Barnes & Siobhan Gorman, *Cyberwar Plan Has New Focus On Deterrence*, WALL ST. J., July 15, 2011, at A5. ("Mr. Lynn said a 'foreign intelligence service' had stolen 24,000 files from a U.S. defense contractor in a March [2011] cyber attack.").

[91] *Id.*

[92] *See generally Iranian Cyber Threat to the U.S. Homeland: Joint Hearing Before the Subcomm. on Counterterrorism and Intelligence and the Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs. of the H. Comm. on Homeland Sec.*, 112th Cong. (2012).

[93] *See generally* JOHN O. BRENNAN, CENTRAL INTELLIGENCE AGENCY (Jan. 05, 2016), https://www.cia.gov/about-cia/leadership/john-o-brennan.html.

challenge to our nation and to our critical infrastructure in particular."[94] Mr. Brennan continues:

> What we're seeing now is a lot of intrusions. We're seeing a lot of exfiltrations . . . [T]hen the next step is . . . the disruptive, disabling, destructive types of attacks. And so . . . electric grids, water treatment facilities, . . . mass transportation systems, . . . railways and trains, whatever - if those intruders get into those systems and then can determine how they can in fact interfere in the command and control systems of these systems, they . . . could . . . put trains onto the same tracks. They can . . . bring down electric grids.[95]

In his prepared statement for testimony before the U.S. Senate Intelligence Committee, James Clapper, Director of National Intelligence, stated, "[l]ooking back over my more than half a century in intelligence I have not experienced a time when we've been beset by more crises and threats around the globe. My list is long."[96] Chinese hackers during March 2014 successfully breached the U.S. Office of Personnel Management computers and stole highly sensitive employee files.[97] By May 2014, the U.S. Department of Justice charged five Chinese hackers, identified as officers of Unit 61398 of the Third Department of the Chinese People's Liberation Army ("PLA"), with cyber espionage directed at six American companies: Alcoa, Allegheny Technologies Inc., U.S. Steel, Westinghouse Electric Co., U.S. subsidiaries of

---

[94] Ritika Singh, *Transcript of John Brennan's Speech on Yemen and Drones,* LAWFARE (Aug. 8, 2012), http://www.lawfareblog.com/2012/08/transcript-of-john-brennans-speech-at-the-council-on-foreign-relations/.

[95] *Id.*

[96] *Opening Statement to Worldwide Threat Assessment Hearing: Hearing Before the S. Armed Servs. Comm.*, 113th Cong. (2014) (statement by James R. Clapper, Director of National Intelligence), https://icontherecord.tumblr.com/post/74958293225/remarks-as-delivered-by-james-r-clapper-director.

[97] *See* Matt Apuzzo, *Chinese Businessman is Charged in Plot to Steal U.S. Military Data*, N.Y. TIMES (July 11, 2014), http://www.nytimes.com/2014/07/12/business/chinese-businessman-is-charged-in-plot-to-steal-us-military-data.html?_r=1.

SolarWorld AG, and others.[98] According to the DOJ, "[t]his is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking."[99]

By late 2014, Secretary of Homeland Security Jeh C. Johnson cautioned that in their daily lives, Americans are finding that "cyberspace is vulnerable to an ever-evolving range of threats."[100] Secretary Johnson further observes that this vulnerability stems "from criminals to nation-state actors, ranging in purpose from identity and data theft to espionage and disruption of critical functions. As our Nation's reliance on cyber networks has grown, incidents which impact the safety and confidence with which we operate online have become increasingly commonplace."[101]

By early 2015, James F. Kurose, Assistant Director of the National Science Foundation's (NSF) Corporate and Information Science and Engineering Directorate warned that "[k]ey aspects of business operations, our financial systems, manufacturing supply chains, and military communications are tightly networked, integrating the economic, political, and social fabric of our global society."[102] Vulnerabilities can result from these interdependencies and "lead to a wide range of threats that challenge the security,

---

[98] *See* Press Release, U.S. Dep't. of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

[99] *Id.* (quoting U.S. Attorney General Eric Holder).

[100] Jeh C. Johnson, *Let's Pass Cybersecurity Legislation,* THE HILL (Sept. 9, 2014), http://thehill.com/opinion/op-ed/217151-lets-pass-cybersecurity-legislation.

[101] *Id.*; *see also* Daniel Garrie & Shane R. Reeves, *So Your're Telling Me There's a Chance: How the Articles on State Responsibility Could Empower Corporate Responses to State-Sponsored Cyber Attacks,* HARV. NAT'L SEC. J. FEATURES (Dec. 17, 2015); Alan W. Ezekiel, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft,* 26 HARV. J. L. & TECH. 649 (2013); Xiang Li, *Hactivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime,* 27 HARV. J. L. & TECH. 301 (2013).

[102] *The Expanding Cyber Threat: Hearing Before the Subcomm. On Res. & Tech. of the H. Comm. on Sci., Space & Tech.*, 114th Cong. (2015) (statement of James F. Kurose, Assistant Director, Computer and Information Science and Engineering Directorate, National Science Foundation).

reliability, availability, and overall trustworthiness of all systems and resources rooted in information technology. Coupled with Internet adoption patterns, we are witnessing a dramatic shift in the size, complexity, and diversity of cyber security attacks."[103] Before Congress, Kurose testified that the United States:

> Needs to continue its investments in game-changing research if our cyber systems are to be trustworthy now and in the future. As you know, every day, we learn about more sophisticated and dangerous attacks. Why is the cyber security challenge so hard? The general answer is that attacks and defenses co-evolve: a system that was secure yesterday might no longer be secure tomorrow. More specific responses to this question include:
>
> • The technology base of our critical infrastructure systems is frequently updated to improve functionality, availability, and/or performance. New systems introduce new vulnerabilities (unknowable in the lab) that need new defenses when put into practice.
>
> • The environments in which our computing systems are rapidly developed and deployed, and the functionality that they provide are also not static. With entirely new computing models/platforms, like cloud and mobile computing, come new content and function, which in turn create new opportunities and incentives for attack and disruption.
>
> • As the automation of complex system interdependencies comes to pervade our critical infrastructure, new kinds of cascading vulnerabilities can be accidentally created and subsequently discovered in these systems, including the electric power grid, automated transportation networks, and robotic medical systems.
>
> • The sophistication of attackers is increasing as well as their sheer number and the specificity of their targets.
>
> • As information and systems are increasingly connected, and are increasingly composed of software and hardware

[103] *Id.*

> produced by global supply chains, the opportunities for malicious insiders to cause damage increases, and the risks of information leaks multiply.
>
> • As more systems and data become accessible, information that was once low risk becomes high risk through correlation that was unimaginable only a few years ago.
>
> • Achieving system trustworthiness is not purely a technology problem. System developers, purchasers, operators and users all have a role to play in system security, and ways to incentivize positive behaviors are required. Security mechanisms that are not convenient will be circumvented; security mechanisms that are difficult to understand will be ignored or misinterpreted. Indeed, cyber security is a multi-dimensional challenge, requiring expertise in computer science, mathematics, economics, behavioral sciences, and education.[104]

In Congressional testimony given on March 4, 2015, Navy Admiral Michael S. Rogers, commander of the U.S. Cyber Command and director of the National Security Agency, stated:

> Every conflict in the world today has a cyber dimension . . . . The most worrisome of these campaigns are state-sponsored, persistent, and worldwide in scope. They are aimed at governments, non-profits, and corporations wherever they might be accruing intellectual capital that the attackers believe could be valuable, whether for re-sale or passage to competing firms and industries . . . . We see states developing capabilities and attaining accesses for potential hostilities, perhaps with the idea of enhancing deterrence or as a beachhead for future cyber sabotage. Private security researchers over the last year have reported on numerous malware finds in the industrial control systems of energy sector organizations . . . . We believe potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that

[104] *Id.*

> our homeland is at risk if tensions ever escalate toward military conflict.[105]

Time and time again, specific warnings have been presented to Congress about what needs to be done by government and private organizations to increase their cybersecurity defenses. Secretary of Defense Ash Carter cautioned, "The same Internet that enables Wikipedia also allows terrorists to learn how to build a bomb. And the same technologies we use to target cruise missiles and jam enemy air defenses can be used against our own forces—and they're now available to the highest bidder."[106] Vice Chairman of the Joint Chiefs of Staff, Navy Admiral James A. Winnefeld, Jr. said, "Today, 96 percent of our most advanced electronic warfare systems are assembled with commercially available components. We only add 4 percent worth of 'special sauce."[107] That means adversaries can quickly copy advanced U.S. systems with globally sourced components."[108] Ash Carter warned that "[w]hether it's in the cloud, infrared cameras, or the GPS signals that provide navigation for ride-sharing apps, but also for aircraft carriers and our smart bombs—our reliance on technology has led to real vulnerabilities that our adversaries are eager to exploit."[109]

Secretary of Defense, Ash Carter, explains nation-states, terrorist, and criminal networks are "increasing their cyber operations. Low-cost and global proliferation of malware have lowered barriers to entry and made it easier for smaller malicious actors to strike in cyberspace. We're also seeing blended state-and-non-state threats in cyber . . . which complicates potential

---

[105] *Cyber Operations: Improving the Military Cybersecurity Posture in an Uncertain Threat Environment: Hearing Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Servs.*, 114th Cong. (2015) (statement of Admiral Michael S. Rogers, Commander, U.S. Cyber Command and Director, National Security Agency).

[106] Ash Carter, United States Sec'y of Def., Drell Lecture: Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity (Apr. 23, 2015).

[107] Jim Garamone, *Winnefeld: DoD Must Strengthen Public, Private Ties*, DOD NEWS (2015), http://www.defense.gov/news/newsarticle.aspx?id=128810.

[108] *Id.*

[109] *See* Carter, *supra* note 106.

responses for us and for others."[110] The long list of top U.S. government officials echoing these warnings includes Francis X. Taylor, Under Secretary for the Office of Intelligence and Analysis at the Department of Homeland Security. He stated, "[T]errorist groups operating in permissive environments present a significant security threat to the U.S. and our allies . . . . [T]he terrorist threat is fluid and cannot be associated with one group, race, ethnicity, national origin, religion, or geographic location."[111] And, as DHS's Andy Ozment, Assistant Secretary for Cybersecurity and Communications, stated, "[U]ltimately, there exists no perfect cyber defense, and persistent adversaries will find ways to infiltrate networks in both government and the private sector."[112]

Cyberattack: A National Security Issue

"The next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems," observed Central Intelligence Agency Director Leon Panetta in his June 9, 2011 confirmation hearing for the post of Secretary of Defense before the Senate Armed Services Committee.[113] A Wall Street Journal article titled *Cyber Combat: Act of War*, observed "[t]he Pentagon's first formal cyber strategy

---

[110] *See id.*

[111] *Terrorism Gone Viral: The Attack in Garland, Texas and Beyond: Hearing Before the H. Comm. on Homeland Sec.*, 114th Cong. (2015) (statement by Francis X. Taylor, Under Secretary, Office of Intelligence and Analysis, U.S. Dept. of Homeland Security).

[112] *DHS' Efforts to Secure Gov: Hearing Before the Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs. of the H. Comm. on Homeland Sec.*, 114th Cong. (2015) (witness statement of Andy Ozment, Assistant Secretary for Cybersecurity and Communications).

[113] Anna Mulrine, *CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyberattack,* THE CHRISTIAN SCIENCE MONITOR (June 9, 2011), http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack; *see also* Eric Talbot Jensen, *President Obama and the Changing Cyber Paradigm,* 37 WM. MITCHELL L. REV. 5049 (2011); Stuart Malawer, *Cyberwarfare: Law & Policy Proposals for U.S. & Global Governance,* 58 VA. LAWYER 28 (2010) (GMU School of Public Policy Research Paper No. 2009-11, http://ssrn.com/abstract=1437002); Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,* 27 BERKELEY J. INT'L L. 192 (2009).

. . . represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military." [114]

The analogy of a cyberattack scenario to Pearl Harbor is not unique to Leon Panetta or this article. Nearly two decades ago, defense analysis professor John Arquilla describes "the first global cyberwar, where the enemy is invisible, the battles virtual, and the casualties all too real."[115] Arquilla's fictional day-by-day detailed depiction of a three-week-long cyber assault and its precipitating events remains a great read, and with very few exceptions, is just as contemporary today. In 2012, Mike McConnell, former director of national intelligence during President George W. Bush's administration, warned, "the United States could not 'wait for the cyber equivalent of the World Trade Centers.'"[116]

The USA PATRIOT Act[117] defines *critical infrastructure* as "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."[118] Presidential Decision Directive 63 (or PDD-63)

---

[114] Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, at A1.

[115] John Arquilla, *The Great Cyberwar of 2002,* WIRED 122 (Feb. 1, 1998, 12:00 PM), http://archive.wired.com/wired/archive/6.02/cyberwar_pr.html; *see also Hearings On Security in Cyberspace, Before the Perm. Subcomm. On Investigations of the S. Comm. on Govt. Affairs*, 104th Cong. (1996) (statement of Jamie S. Gorelick, Deputy Attorney General), https://ia802708.us.archive.org/11/items/securityincybers00unit/securityincybers00unit_bw.pdf (last viewed Apr. 12, 2016) (observing "There are skeptics who have said that the nation will have to endure the cyber equivalent of Pearl Harbor . . . before the government and industry wake up to the problem of protecting our critical infrastructures from the new cyber threats.").

[116] *See* Thomas Rid, *supra* note 69, at 77.

[117] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, P.L. 107-56.

[118] *See id.* at § 1016(e); Homeland Security Presidential Directive No. 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003) (describing the asset loss impact level necessary to deem the asset as "critical."). *See also* RITA TEHAN, CONG. RESEARCH SERV., R44410,

identified the requirement to protect the following critical infrastructures: "information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production; and storage."[119] The following four activities controlled by the federal government were specifically identified by PDD-63: "internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense." [120] During February 2013, the Obama Administration issued PPD-21, *Critical Infrastructure Security and Resilience* thus superseding HSPD-7.[121]

By 2016, Jessica Stern's chilling synopsis is that "[c]ivil war, sectarian tensions, and state failure in the Middle East and Africa ensure that Islamist terrorism will continue its spread in those regions − and most likely in the rest of the world as well."[122] The emergence of the self-proclaimed Islamic State (known as ISIS) is perhaps the most troubling threat to world peace, "a protean Salafi jihadist organization whose brutal violence, ability to capture and hold territory, significant financial resources, and impressive

---

CYBERSECURITY: CRITICAL INFRASTRUCTURE AUTHORITATIVE REPORTS AND RESOURCES 1 (2016). This included causing catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction; impairing federal agencies' abilities to perform essential missions or ensure the public's health and safety; undermining state and local government capacities to maintain order and deliver minimum essential public services; damaging the private sector's capability to ensure the orderly functioning of the economy; having a negative effect on the economy through cascading disruption of other infrastructures; or undermining the public's morale and confidence in our national economic and political institution. HSPD-7 has since been superseded by PDD-21.

[119] *See* RITA TEHAN, supra note 118, at 1.

[120] *Id.*

[121] *Id.* (*citing Critical Infrastructure Security and Resilience*, THE WHITE HOUSE, Feb. 12, 2013 at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. (last visited Mar. 25, 2016)).

[122] Jessica Stern, *Obama and Terrorism: Like It or Not, the War Goes On*, FOREIGN AFF., Sept.–Oct. 2015, at 62.

strategic acumen make it a threat unlike any other the United States has faced in the contemporary era."[123]

Going Dark

Central to creating effective cyberattack policy is addressing the tension surrounding the debate about privacy. FBI Director James B. Comey[124] describes the controversial problem known as "going dark" to the Senate Judiciary Committee as "the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant."[125] In testimony given to the Senate Select Committee on Intelligence, Director Comey observes that we "live in a technologically driven society and just as private industry has adapted to modern forms of communication so too have the terrorists. Unfortunately, changing forms of internet communication are quickly outpacing laws and technology designed to allow for the lawful intercept of communication content."[126]

Law Professor Peter Swire reports that the Review Group, having full awareness of concerns about the "going dark" controversy, "sharply criticized any attempt to introduce vulnerabilities into commercially available products and services, and found that even temporary vulnerabilities should be authorized only after administration-wide scrutiny."[127] Moreover, based on

---

[123] *Id.*

[124] FBI Executives: Director James Comey, FBI, https://www.fbi.gov/about/leadership-and-structure/fbi-executives.

[125] *Going Dark: Encryption, Tech., and the Balance Between Pub. Safety and Privacy: Hearing Before the S. Judiciary Comm.,* 114th CONG. (2015) (Joint Statement By James B. Comey, Director, Federal Bureau of Investigation with Deputy Attorney General Sally Quillian), http://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy.

[126] *Counterrorism, Counterintelligence, and the Challenges of Going Dark*, 114th CONG. (2015) (Statement By James B. Comey, Director, Federal Bureau of Investigation), http://www.intelligence.senate.gov/hearings/counterterrorism-counterintelligence-and-challenges-going-dark.

[127] *Going Dark: Encryption, Tech., and the Balance Between Pub. Safety and Privacy: Hearing Before the S. Judiciary Comm.,* 114th CONG. (2015)

substantial experiences of the Review Group and following top-secret briefings, it was the Group's clear and unanimous recommendation that strong encryption be encouraged, finding "these policies would best fight cyber-crime, improve cybersecurity, build trust in the global communications infrastructure, and promote national security."[128]

V. ROADMAP TO TRAGEDY

"We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation space systems."

Hon. James R. Clapper
Director of National Intelligence
February 9, 2016 [129]

Cyber attacks continue to escalate and progressively appear war like in nature.

Governance of Cyber Conflict

Continued rapid worldwide adoption of the Internet, mobile phone service, technological advances, and increased interconnectivity results in needed accommodations in law for acts of cyber conflict.[130] Kristen Eichensehr contends that nation states

---

(Statement By Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology) (Professor Swire has worked for more than two decades on encryption issues as a scholar, government official, and as a member of President Obama's Review Group on Intelligence and Communications Technology, http://www.techpolicy.com/Blog/February-2016/Peter-Swire-Says-It-s-a-Case-of-National-Security.aspx).

[128] *Id.*

[129] *Worldwide Threat Assessment Hearing: S. Select Comm. on Inte'l*., 115th CONG. (2016) (statement of Hon. James R. Clapper, Director of National Intelligence, http://www.dni.gov/files/documents/2016-02-09SSCI_open_threat_hearing_transcript.pdf.

[130] *See generally* Laurie R. Blank, *Cyberwar/Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace, in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS (Oxford University Press 2014); Lianne J.M. Boer, *Restating the Law 'As It Is': On the Tallinn Manual and the*

have been required to answer the following three fundamental questions for other domains, and they must now be answered for cyber: "(1) what role, if any, private parties should play in

Use of Force in Cyberspace, 5 AMSTERDAM L. FORUM (2013); Lianne J.M. Boer & Arno R. Lodder, Cyberwar: What Law to Apply? And to Whom?, Chapter 10 Cyberwar, *in* CYBER SAFETY: AN INTRODUCTION, Eleven Publishing (Rutger Leukfeldt & Wouter Stole eds., 2012); Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J. L. SCI. & TECH. 137 (2013); Myriam Dunn Cavelty, The Militarisation of Cyber Security as a Source of Global Tension, *in* STRATEGIC TRENDS ANALYSIS, Zurich, Möckli, Daniel, Wenger, Andreas, eds., Center for Security Studies (2012); Kristen Eichensehr, *Cyberwar & International Law Step Zero,* 50 TEX. INT'L L.J. 355 (2015); Carol M. Hayes & Jay P. Kesan, *Law of Cyber Warfare, in* INTERNATIONAL ENCYCLOPEDIA OF DIGITAL COMMUNICATION AND SOCIETY (Wiley-Blackwell, 2014); Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense,* 32 B. C. INT'L & COMP. L. REV. 439 (2009); Duncan B. Hollis, *New Tools, New Rules: International Law and Information Operations*, *in* THE MESSAGE OF WAR: INOFORMATION, INFLUENCE AND PERCEPTION IN ARMED CONFLICT, G. David and T. McKeldin, eds. (2008); Duncan B. Hollis, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?, in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS (J. Ohlin et al., eds., Oxford University Press 2014); James Kraska & Brian T. O'Donnell, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, 8 J. CONFLICT & SEC. L. 133 (2003); Stuart Malawer, *Cyberwarfare: Law & Policy Proposals for U.S. & Global Governance*, 58 VA. LAWYER 28 (2010); Jeremy Rabkin & John Yoo, *A Return to Coercion: International Law and New Weapons Technologies,* 42 HOFSTRA L. REV. 1187 (2014); John C. Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield* (2011); Peter Swire, *The System of Foreign Intelligence Surveillance Law,* 72 GEO. WASH. L. REV. (2004); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works,* 5 JOURNAL OF LAW AND CYBER WARFARE 147 (2016); Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire,* 8 J. STRATEGIC & INT'L STUD. 105 (2013); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance,* 29 JOHN MARSHALL J. COMPUTER & INFO. L. 313 (2011); Brandon G. Valeriano & Ryan Maness, *The Dynamics of Cyber Conflict between Rival Antagonists*, 2001-2011 (2013); Kristin Westerhorstmann, Note, *The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Attacks, Fake Dating Profiles, and Employees Who Check Facebook at Work,* 5 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 145 (2015); Christopher S. Yoo, *Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures*, CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Jens David Ohlin, Kevin Govern, Claire Finkelstein, eds., 2015).

governance; (2) how the domain should be governed (no governance system, treaty, or norms); and (3) whether and how to regulate military activities in the domain."[131] Professor Eichensehr suggests that the requirements for cyber may differ in important ways from the older schematic of "multilateral governance, governance by treaty, and some level of demilitarization."[132] Calls for greater cyber deterrence among nations also make for a controversial contemporary debate.[133] The tension between national security requirements and privacy issues remain tense.[134]

---

[131] Kristen Eichensehr, *The Cyber-Law of Nations,* The Cyber-Law of Nations, 103 GEO. L.J. 317, 317 (2015).

[132] *Id.*; *see also* SHANE R. REEVES & DAVID A. WALLACE, MODERN WEAPONS AND THE LAW OF ARMED CONFLICT, IN U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 41, 41–66 (Corn, VanLandingham, & Reeves eds., Oxford University Press 2015); Lori Fossum, Cyber Conflict Bibliography, 2015 Update, GWU Law School Public Law Research Paper No. 2015-57; GWU Legal Studies Research Paper No. 2015-57, http://ssrn.com/abstract=2704395.

[133] *See generally* Samantha Bradshaw, *Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity,* Global Commission on Internet Governance Paper Series, Paper no. 23 (2015), http://ssrn.com/abstract=2700899; Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11.2 I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (2015); Robin Geiss & Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention,* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE. INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY, TALLINN (K. Ziolkowski ed., 2014); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 374 (2011); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J. L. & TECH. 429 (2012); Orla Lynskey, LSE Law Department Briefings on the Investigatory Powers Bill - Beyond Privacy: The Data Protection Implications of the IP Bill (Dec. 16, 2015). LSE Law - Policy Briefing Paper No. 2704299, http://ssrn.com/abstract=2704299; Tim Stevens, *A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,* 33 CONTEMP. SEC. POL'Y 148 (2012), http://ssrn.com/abstract=2100764; Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?,* 89 INT'L L. STUD. 252 (2013); K. A. Taipale, *Cyber-Deterrence*, LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION, WARFARE, DIGITAL AND INTERNET IMMOBILIZATION, IGI Global (2010), http://ssrn.com/abstract=1336045.

[134] Jeffrey S. Brand, *Eavesdropping on Our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the*

The Attribution Problem

In the case of many cyberattacks, attribution with certainty to the source of attack is problematic. Brandon Valeriano and Ryan Maness state that "one of the advantages of a cyber dispute is deniability . . . For some cases, attribution is easy; for example, India and Pakistan have been immersed in 'tit for tat' cyber incidents for some time and it is fairly clear that actions in this arena are state sponsored."[135] Professor Michael J. Glennon

---

Surveillance Crisis, 6 HARV. J. NAT'L SEC. (2015), http://ssrn.com/abstract=2562099; Eldar Haber, *The Cyber Civil War*, 44 HOFSTRA L. REV. 41 (2015), http://ssrn.com/abstract=2699644; Andrew Hilts & Christopher A. Parsons, *Half Baked: The Opportunity to Secure Cookie-Based Identifiers from Passive Surveillance* (2015), http://ssrn.com/abstract=2640610; Joanna Kulesza, *USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining?,* 2 GRONINGEN J. INT'L L. (2014), http://ssrn.com/abstract=2599274; Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet,* 66 STAN. L. REV. (2013), http://ssrn.com/abstract=2628412; Joel R. Reidenberg, *The Transparent Citizen*, 47 LOY. U. CHI. L.J. (2015), http://ssrn.com/abstract=2674313; Dakota S. Rudesill, *Coming to Terms with Secret Law,* 7 HARV. NAT'L SEC. J. (2015), Forthcoming, http://ssrn.com/abstract=2687223; Shaun B. Spencer, *When Targeting Becomes Secondary: A Framework for Regulating Predictive Surveillance in Antiterrorism Investigations,* 92 DENVER U. L. REV. 493 (2015), http://ssrn.com/abstract=2694615; Cass R. Sunstein, *Beyond Cheneyism and Snowdenism*, 83 U. CHI. L. REV. 271 (2016), http://ssrn.com/abstract=2589636; Laura Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, BUS. L. REV. (Forthcoming), http://ssrn.com/abstract=2563573; Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, Georgia Tech Scheller College of Business Research Paper No. #36, http://ssrn.com/abstract=2709619; Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection,* 90 N. C. L. REV. (2012), http://ssrn.com/abstract=1989516; Peter Swire, *The Second Wave of Global Privacy Protection: Symposium Introduction,* 74 OHIO ST. L.J. (2013), http://ssrn.com/abstract=2404261; Peter Swire, *Finding the Best of the Imperfect Alternatives for Privacy, Health IT, and Cybersecurity,* 2013 WIS. L. REV. 649 (2013), http://ssrn.com/abstract=2187305; Peter Swire, *The Uses and Limits of Financial Cryptography: A Law Professor's Perspective,*1318 LECTURE NOTES IN COMP. SCI. 239 (1997), *http*://ssrn.com/abstract=11473; Jeffrey L. Vagle, *Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance*, 90 IND. L.J. (2015), http://ssrn.com/abstract=2550934.

[135] Brandon G. Valeriano & Ryan Maness, *The Dynamics of Cyber Conflict between Rival Antagonists*, 2001-2011, 9 (2013), http://ssrn.com/abstract=2214332.

observes that "[i]f cyber activity and its sponsor are concealed . . . and verification and compliance is impossible, so too is deterrence and effective legal regulation. No verifiable international agreement can regulate the covert writing or storage of computer code useful for launching a clandestine cyber attack."[136] The anonymous nature of the internet complicates effective deterrence because "[t]o attribute a cyber attack to a state, it's necessary to establish what computer was used, who was sitting at the computer (if it's not government owned), and what government or organization that person worked for . . . concealment is baked into the structure of the Internet [and not feasibly] . . . eliminated."[137]

Clear and Present Danger

Today's information warfare campaigns utilize malicious information gathering software, denial of service attacks, some highly sophisticated targeted cyberweapons like Stuxnet, and espionage and data exfiltration attacks.[138] Julie J.C.H. Ryan warns that "[t]he use of malicious software to encrypt large blocks of data for denial is possible and could have devastating consequences, removing en masse capabilities for control and coordination as relevant information is rendered inaccessible."[139]

---

[136] Michael J. Glennon, *The Dark Future of International Cybersecurity Regulation,* 6 J. NAT'L SEC. L. & POL'Y 563 (2013), *citing* Patrick M. Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm, in* NATIONAL ACADEMY OF SCIENCES, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 55 (2010); Mike McConnell, *To Win the Cyber War, Look to the Cold War,* WASH. POST, Feb. 28, 2010, at B1.

[137] Glennon, *supra* note 136, at 566–67, *citing* David D. Clark & Susan Landau, *Untangling Attribution,* 2 HARV. NAT'L SEC. J. 531 (2011) ("The Internet was not designed with the goal of deterrence in mind . . . ."); Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare,* 97 J. CRIM. L. & CRIMINOLOGY 379 (2007) (discussing how attribution is complicated by computer technology); Elizabeth Hanford, *The Cold War of Cyber Espionage,* 20 PUB. INTEREST L. RPTR. 22 (2014); Jens David Ohlin, *Cyber-Causation, in* CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS, Jens David Ohlin, Claire Finkelstein, and Kevin Govern, eds., Oxford University Press (2015), http://ssrn.com/abstract=2488130.

[138] *See* JULIE J. C. H. RYAN, *supra* note 66, at 6.

[139] *Id.*

Director of National Intelligence James Clapper states that "2014 saw, for the first time, destructive cyber attacks carried out on U.S. soil by nation state entities, marked first by the Iranian attack against the Las Vegas Sands Casino Corporation . . . and the North Korean attack against Sony in November [2014]."[140] While many believe that both Iran and North Korea possess lesser technical capabilities than either China or Russia, "these destructive attacks demonstrate that Iran and North Korea are motivated and unpredictable cyber actors."[141] Recently, "[n]onstate actors have increasingly used information technologies to create the connectivity, and thus the unifying motivation, for their community of influence. Virtual non-state actors, such as Anonymous, have emerged that exist in online venues and operate primarily in the information domain."[142] Larisa Breton concludes, "virtual non-state actors have the potential to affect both warfare and governance."[143]

FBI Director James Comey testified before Congress on July 8, 2015 that "millions and millions of U.S. government background-investigation records—dating back 20 years—were stolen by hackers who broke into the Office of Personnel Management's ("OPM") network."[144] Chairman Jason Chaffetz of the House Committee on Oversight and Government Reform characterized the OPM breach as "one of the biggest data breaches in our country's history . . . [and remarked that] [o]nly the imagination

---

[140] Worldwide Threat Assessment Hearing: S. Armed Services Comm., 114th Cong. (2015) (statement of Hon. James R. Clapper, Director of National Intelligence, http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee (last visited Apr. 13, 2016); Lawrence J. Trautman, *The SONY Data Hack: Implications for World Order,* 5 J.L. CYBER WARFARE 1 (forthcoming) (on file with author).

[141] *Id; see also* Yadron, *supra* note 38.

[142] Julie J. C. H. Ryan, *supra* note 66.

[143] Larisa Breton, *Virtual NonState Actors as Clausewitzian Centers of Gravity: An Examination for Sensemaking, Elaboration, and Discussion*, In JULIE J. C. H. RYAN, LEADING ISSUES IN INFORMATION WARFARE AND SECURITY RESEARCH VOL. 2, APCIL (2015).

[144] Damian Paletta, *Personnel Data Breach A 'Huge Deal,'* WALL ST. J., July 9, 2015, at A3.

limits what a foreign adversary could do with detailed information about a federal employee's education, career, health, family, friends, neighbors, and personal habits."[145] Jane Harmon is a former nine-term member of the U.S. House of Representatives, representing California and served as the Ranking Democratic Member on the U.S. House Intelligence Committee from 2002 to 2006. Former Congresswoman Harmon wrote during 2015 that, "[s]urprise developments . . . have blindsided U.S. officials. The disintegration of Syria, the Boston Marathon bombing, the precipitous rise of the Islamic State of Iraq and . . . ("ISIS"), the systematic hacking of U.S. computer networks—in one way or another, all caught Washington flat-footed."[146]

Chairman Ron Johnson of the Senate Homeland Security and Governmental Affairs Committee observed that "in 2003, a cascading failure across the grid in the Northeast left almost 50 million people without power, many for days. One federal study identified nine critical substations that could be disabled and potentially bring down the entire U.S. grid for more than 18 months."[147] In his July 22, 2015 Congressional testimony, Former Director of Central Intelligence, Ambassador R. James Woolsey, warned that:

> Ignorance of the military doctrines of potential adversaries and a failure of strategic imagination is setting America up for an EMP [electromagnetic pulse] Pearl Harbor that could easily be avoided-if we would only heed that terrorist sabotage of electric grids and cyber-attacks are early warning indicators. In fact, in the military doctrines,

---

[145] OPM Data Breach: Part II: Hearing Before the H. Comm. on Oversight and Government Reform, 114th Cong. 2–3 (2015) (statement of Jason Chaffetz, Chairman, H. Comm. on Oversight and Government Reform).

[146] *See* Jane Harman, *Disrupting the Intelligence Community: America's Spy Agencies Need an Upgrade*, FOREIGN AFF., Mar.–Apr. 2015, at 99.

[147] *Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse: Hearing Before the S. Homeland Sec. and Governmental Affairs Comm.*, 114th Cong. (2015), http://www.hsgac.senate.gov/hearings/protecting-the-electric-grid-from-the-potential-threats-of-solar-storms-and-electromagnetic-pulse (opening statement of Ron Johnson, Chairman, S. Homeland Sec. and Governmental Affairs Comm.).

> planning, and exercises of Russia, China, North Korea and Iran, nuclear EMP attack is the ultimate weapon in an all-out cyber operation aimed at defeating nations by blacking-out their electric grids and other critical infrastructures.[148]

Aircraft control system vulnerabilities create the possibility of targeted air system grinding to a halt, resulting in exclusive air supremacy for an aggressor and a significant change in the balance of power.[149] Reports from *The Washington Post* during early 2016 depict hackers creating a Ukraine power outage during the holiday season, creating a troubling escalation of digital attacks.[150] Michael J. Assante contends that "[a] small number of sources in Russia and Ukraine indicate the electrical outage was caused by a cyber attack, specifically a virus from an outside source. I am skeptical as the referenced outage has been hard to substantiate and the cause surfaced relatively quickly."[151] Assante is dubious because "normally, determining root cause analysis of an incident takes time especially when it pertains to activity on the network."[152] Elsewhere, the Computer Emergency Response Team of Ukraine ("CERT-UA") "confirms reports that the BlackEnergy espionage

---

[148] *Id.* (statement of Ambassador R. James Woolsey, Chairman, Foundation for Defense of Democracies, Former Director of Central Intelligence).

[149] *See* JULIE J. C. H. RYAN, *supra* note 66, at 7 (citing Kim Zetter, *Feds Say that Banned Research Commandeered a Plane,* WIRED (May 15, 2015, 10:14 PM), http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/ (last viewed Apr. 13, 2016).).

[150] *See* Andrea Peterson, *Hackers Caused a Blackout for the First Time, Researchers Say,* WASH. POST (Jan. 5, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/; *see also* Jay P. Kasan & Carol Mullins Hayes, Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities (Feb. 20, 2016) (unpublished paper), *http://ssrn.com/abstract=2739894.*

[151] *See* Michael J. Assante, *Current Reporting on the Cyber Attack in Ukraine Resulting in Power Outage,* SANS INDUS. CONTROL SYS. BLOG (Dec. 30, 2015), https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage; *see also* Robert M. Lee, *Potential Sample of Malware from the Ukraine Cyber Attack Uncovered,* SANS INDUS. CONTROL SYS. BLOG (Jan. 1, 2016), https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered.

[152] *Id.*

Trojan—and KillDisk wiper malware—infected systems of the hacked energy supplier, which suffered a three-hour electricity blackout on Dec. 23, [2015] after multiple electrical substations went offline, leaving about 1.4 million homes in the country's western Ivano-Frankivsk region without power."[153]

Cyber "War Games" Conducted

In July 2015, the *Wall Street Journal* reported that the "Pentagon, Department of Homeland Security, National Security Agency and a host of other agencies joined British officials and a number of private companies for a three-week cyberwar game, testing 14 teams on a range of simulated attacks on two continents."[154] Practicing crisis situation scenarios is a basic strategy of good enterprise governance.[155] These types of practice exercises and vulnerability testing often produce valuable lessons.

Impact of Technological Change

According to Frank Cilluffo, the growing pace of cyberattacks "is magnified by the speed at which technologies continue to evolve and by the fact that our adversaries continue to adapt their tactics, techniques and procedures in order to evade and defeat our prevention and response measures."[156] This means that the likelihood of cyberattack increases on almost a daily basis due to technological advances in big data;[157] brain-computer interfaces;[158]

---

[153] *See* Mathew J. Schwartz, *Ukrainian Power Grid Hack: 9 Questions,* BANK INFO SEC. (Jan. 6, 2016), *http://www.bankinfosecurity.com/ukrainian-power-grid-hack-9-questions-a-8781*.

[154] Damian Paletta, *Private Firms Join Cyberattack Exercise,* WALL ST. J., July 6, 2015, at A3.

[155] *See generally* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. (forthcoming 2016), http://ssrn.com/abstract=2623219.

[156] *A Global Perspective on Cyber Threats: Hearing Before the Subcomm. On Oversight and Investigations of the H. Comm. on Fin. Services*, 114th Cong. (2015) (statement of Frank J. Cilluffo, Director, Center for Cyber and Homeland Security, George Washington U.).

[157] *See generally* BENOIT DUPONT, THE CYBER SECURITY ENVIRONMENT TO 2022: TRENDS, DRIVERS AND IMPLICATIONS (2012), http://ssrn.com/abstract=2208548.

code and encryption;[159] cloud computing;[160] cyber weapons;[161] face recognition surveillance;[162] internet of things;[163] military weapons;[164] mobile internet;[165] quantum computing;[166] sensor

---

[158] *See generally* Michelle A. Scheinman, Protecting Your Brain Waves and Other Biometric Data in a Global Economy (Apr. 8, 2013) (unpublished paper), http://ssrn.com/abstract=2382951.

[159] *See generally* Arno R. Lodder, *When 'There' Can Be Everywhere: On the Cross-Border Use of WhatsApp, Pandora, and Grindr*, 5 EUR. J. OF L. & TECH. (2014), http://ssrn.com/abstract=2532652; Christopher Marsden & Ian Brown, Regulating Code: Inter-Disciplinary Empirical Case Studies in Governance and Regulation, TPRC 2011 (2011), http://ssrn.com/abstract=1989676; Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud* (INTERNATIONAL DATA PRIVACY LAW, WORKING PAPER NO. 175, 2012), http://ssrn.com/abstract=2038871.

[160] *See generally* Matthew B. Becker, *Interoperability Case Study: Cloud Computing*, Berkman Center Research Publication No. 2012-11 (2012), http://ssrn.com/abstract=2046987; Paul M. Schwartz, *Information Privacy in the Cloud,* 161 U. PA. L. REV. 1623 (2013), http://ssrn.com/abstract=2290303; Sarah Jane Hughes, *Did the National Security Agency Destroy the Prospects For Confidentiality and Privilege When Lawyers Store Clients' Files in the Cloud — And What, If Anything, Can Lawyers and Law Firms Realistically Do in Response?,* 41 N. KY. L. REV. (2014), http://ssrn.com/abstract=2539609.

[161] *See* Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Review of Cyber Weapons,* 7 J. NAT'L SEC. L. & POL'Y 115 (2014).

[162] *See generally* Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places,* 16 VA. J. L. & TECH. 430 (2011).

[163] *See generally* Eric Barbry, *The Internet of Things, Legal Aspects: What Will Change (Everything) . . . ,* 87 COMM. & STRATEGIES 83 (2012), http://ssrn.com/abstract=2304137; WILLIAM H. DUTTON, THE INTERNET OF THINGS (2013), http://ssrn.com/abstract=2324902; WILLIAM H. DUTTON, ET AL., A ROADMAP FOR INTERDISCIPLINARY RESEARCH ON THE INTERNET OF THINGS: SOCIAL SCIENCES (2013), http://ssrn.com/abstract=2234664.

[164] *See generally* Gary E. Marchant et al., *International Governance of Autonomous Military Robots,* 12 COLUM. SCI. & TECH. L. REV. 272 (2011), http://ssrn.com/abstract=1778424.

[165] *See generally* Navid Hassanpour, Media Disruption Exacerbates Revolutionary Unrest: Evidence from Mubarak's Quasi-Experiment (2011), APSA 2011 Annual Meeting Paper, http://ssrn.com/abstract=1903351; Joshua Goldstein, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution* (2007), Berkman Center Research Publication No. 2007-14, http://ssrn.com/abstract=1077686.

devices;[167] Wi-Fi and wireless;[168] and new technological threats to the global financial system.[169] Charles J. Dunlap warns that when nation state actors engage in the increased proliferation of malicious computer viruses turned loose "on a technology-dependent high-tech society may be as devastating to noncombatants as many of their biological namesakes."[170] Thomas Friedman explains it this way: "But today, when individuals can easily access all the tools of collaboration and superempower themselves . . . individuals do not need to control a country to threaten large numbers of other people. The small can act very big today and pose a serious danger to world order—without the instruments of a state."[171]

Encryption and the "Least Trusted Country" Problem

Stewart A. Baker and Nathan A. Sales state, "[i]nformation policy is a central front in the war on terrorism.[172] In July 2015 testimony before the Senate Judiciary Committee, law professor Peter Swire talked about the vulnerability known as the "least trusted country" problem, where "[i]f one country sets limits on encryption, then cross-border communications that comply with

---

[166] *See generally* BENOIT DUPONT, THE CYBER SECURITY ENVIRONMENT TO 2022: TRENDS, DRIVERS AND IMPLICATIONS (2012), http://ssrn.com/abstract=2208548.

[167] *See generally* Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places,* 59 FLA. L. REV. 1 (2007), http://ssrn.com/abstract=956160.

[168] *See generally* Rob Alderfer, Dirk Grunwald & Kenneth R. Baker, *Toward Expanded Wi-Fi Access in the 5 GHz Band*, U. OF COLO. (2013), http://ssrn.com/abstract=2411683.

[169] *See Generally* Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L. Q. REP. 232 (2016), http://ssrn.com/abstract=2786186; Lawrence J. Trautman & Alvin Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. (2017), http://ssrn.com/abstract=2730983.

[170] Charles J. Dunlap, Jr., The Law of Cyberwar, A Case Study from the Future, in *Cyberwar 2.0: Myths, Mysteries and Realities* 139, 146 (Alan D. Campen & Douglas H. Dearth, eds., 1998).

[171] Friedman, *supra* note 21, at 609.

[172] Stewart A. Baker & Nathan A. Sales, *Homeland Security, Information Policy, and the Transatlantic Alliance*, GEO. MASON L. & ECON. RES. PAPER SERIES 09-20, 2 (2009), http://ssrn.com/abstract=1361943.

that country's laws will have that vulnerability. If one party . . . uses compromised encryption as required in that country, then those globally who communicate with that country will have their communications compromised as well."[173]

This vulnerability is a particular problem because of lax data security in many other parts of the world where U.S.-generated data traffic either passes through or is destined. The significant growth in either the development or maintenance of computer code via business process outsourcing ("BPO") by American companies to businesses located in such countries as India may be a critical weakness leading up to a cyber Pearl Harbor.[174]

VI. WHAT IS TO BE DONE?

"Terrorists will almost certainly continue to benefit . . . from a new generation of recruits proficient in information technology, social media, and online research. Some terrorists will look to use these technologies to increase the speed of their communications, the availability of their propaganda, and ability to collaborate with new partners. They will easily take advantage of widely available, free encryption technology, mobile-messaging applications, the dark web, and virtual environments to pursue their objectives."

Hon. James R. Clapper
Director of National Intelligence
February 9, 2016 [175]

---

[173] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the Senate Judiciary Comm.*, 114th Cong. (2015), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf (statement By Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology).

[174] *See* Scott Shackelford, Scott Russell & Jeffrey Haut, *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks,* U.C. DAVIS BUS. L.J. (forthcoming 2016), http://ssrn.com/abstract=2702039 (comparing similarities and differences between U.S. 2014 National Institute for Standards and Technology (NIST) Cybersecurity Framework with standards and best practices employed by other nations such as Canada and India).

[175] *Worldwide Threat Assessment Hearing: S. Select Comm. on Int'l, 115th Cong*. (2016), https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FI

Professor Julie Ryan contends that among the number of serious geopolitical questions that must be considered include what specific cyberspace conduct "rise[s] to the level of [an] act of armed aggression? Does it matter if these acts are carried out by nations, corporations, ad hoc groups, or individuals? [A]re the asymmetries associated with information warfare so great that unleashing the potential might in fact redraft the geopolitical landscape?"[176] Despite whether their policies toward the Internet are characterized as "open or closed," governments worldwide continue to face "inherent perpetual difficulty in regulating online spaces."[177] Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle and Francesca Spidalieri observe that:

> A sound National Cyber Security Strategy . . . must be actionable. Today, the prime topics reflected in most strategies include: outlining organizational and positional authority within the government; fostering awareness and education among citizens; building an incident and crisis management response capability; expanding law enforcement's capacity to deal with the rate of cyber crimes; facilitating private-public partnerships and developing trusted information sharing exchanges; and

---

NAL.pdf (statement of Hon. James R. Clapper, Director of National Intelligence).

[176] Julie J. C. H. Ryan, LEADING ISSUES IN INFORMATION WARFARE AND SECURITY RESEARCH, xii (2012).

[177] Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?,* 2015 U. ILL. J.L., TECH. & POL'Y 341, 377 (2015), http://ssrn.com/abstract=2548561 (citing Robert Faris & Rebekah Heacock Jones, *Platforms and Policy*, INTERNET MONITOR 2014: REFLECTIONS ON THE DIGITAL WORLD 28, 29 (Urs Gasser et al. eds., 2014)); Hitoshi Nasu & Helen Trezise, *Cyber Security in the Asia Pacific*, ANU College of Law Research Paper 2015 Series 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2700388; Nicholas Tsagourias and Russell Buchan (eds), Research Handbook on International Law and Cyberspace 446–64 (Edward Elgar, 2015); Nazli Choucri, *Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University* (unpublished manuscript) http://ssrn.com/abstract=2727414.

> marshaling resources toward a R&D and innovation agenda.[178]

Daniel J. and Julie J.C.H. Ryan observe "[m]ost corporations would no more consider the need to develop, and pay for, the technologies, practices and procedures that would be needed to defend against a state-sponsored INFOWAR attack than they would develop the technologies, practices and procedures to protect themselves against a strategic exchange of thermonuclear weapons."[179] Robert Faris and Rebekah Heacock Jones observe that during the past decade all governmental

> Core regulatory challenges have changed in degree but not in kind; issues of scale, jurisdiction, and attribution, which are tied to the ability to conduct surveillance, complicate any efforts to regulate online activity. The ability to identify individuals associated with online activity facilitates regulation . . . and mechanisms that allow individuals to cloak their identity or to take refuge outside of their government's jurisdiction reduce regulatory effectiveness.[180]

In their 2014 report by The President's Review Group on Intelligence and Communications Technologies, Richard A. Clarke, Michael J. Stone, Cass R. Sunstein & Peter Swire state that:

> When public officials acquire foreign intelligence information, they seek to reduce risks, above all risks to national security. The challenge, of course, is that multiple risks are involved. Government must consider all of those risks, not a subset, when it is creating sensible safeguards. In addition to reducing risks to national security, public officials must consider four other risks:

---

[178] Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle & Francesca Spidalieri, *Cyber Readiness Index 2.0: A Plan for Cyber Readiness: A Baseline and an Index,* POTOMAC INST. POL'Y STUD. 7 (2015).

[179] Daniel J. Ryan & Julie J.C.H. Ryan, *Protecting the National Information Infrastructure Against Infowar,* 17 COLLOQUY 1, 21-25 (1996).

[180] Robert Faris & Rebekah Heacock Jones, *Internet Monitor 2014: Platforms and Policy*, https://medium.com/internet-monitor-2014-platforms-and-policy/platforms-and-policy-e9984e1be4c6#.hhvpnfuhh.

> · Risks to privacy;
>
> · Risks to freedom and civil liberties, on the Internet and elsewhere;
>
> · Risks to our relationships with other nations; and
>
> · Risks to trade and commerce, including international commerce.[181]

Defense Secretary Ash Carter says, "[d]ozens of militaries are developing cyber forces, . . . and because stability depends on avoiding miscalculation that could lead to escalation, militaries must talk to each other and understand each other's abilities."[182] Admiral Michael S. Rogers observes:

> I liken our historical moment to the situation that confronted the U.S. early in the Cold War, when it became obvious that the Soviet Union and others could build hydrogen bombs and the superpower competition showed worrying signs of instability. We rapidly learned that we needed a nuclear force that was deployed across the three legs of the triad and underpinned by robust command and control mechanisms, far-reaching intelligence, and policy structures including a declared deterrence posture. Building these nuclear forces and the policy and support structures around them took time and did not cause a nuclear war or make the world less safe. On the contrary, it made deterrence predictable, helped to lower tensions, and ultimately facilitated arms control negotiations. While the analogy to cyberspace is not exact, it seems clear that our

---

[181] Richard A. Clarke, Michael J. Stone, Cass R. Sunstein & Peter Swire, THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD xvi (2013).

[182] Cheryl Pellerin, *Carter Unveils New DoD Cyber Strategy in Silicon Valley,* DOD NEWS, U.S. Dept. of Defense (Apr. 23, 2015), http://www.defense.gov/news/newsarticle.aspx?id=128659; *see also* Trey Herr & Drew Herrick, *Military Cyber Operations: A Primer*, 14 AM. FOREIGN POL'Y DEF. TECH. PROG. BRIEF (Jan. 2016), http://ssrn.com/abstract=2725275 (observing that Military Cyber Operations [MCO] is an umbrella term for the acquisition and use of cyber capabilities at the strategic, operational, and tactical levels of conflict); Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252 (2013), http://ssrn.com/abstract=2719034.

> nation must continue to commit time, effort, and resources to understanding our historical situation and building cyber military capabilities, along with the "whole-of-nation" structures and partnerships they work among. Just as we fashioned a formidable nuclear capability that served us through the Cold War and beyond, I am confident in our ability to keep pace with adversaries who are determined to control "their" corners of cyberspace, to exfiltrate our intellectual property, and to disrupt the functioning of our institutions. They are every bit as determined, creative, and persistent in these efforts as the Soviet leaders we contained during the Cold War, and unfortunately we see few hints they will act more responsibly in cyberspace. Thus we must commit to the long-term goal of building a truly open, secure cyberspace governed collaboratively by many stakeholders, while we remain prepared for crises and contingencies that can arise along the way—just as we do in every other domain.[183]

By the end of 2015, Harvard's Jessica Stein observes, "[l]ooking forward, cyberterrorism and cyberwar will likely pose a more serious threat to Americans' well-being than conventional terrorist violence, and government surveillance is and will remain an essential weapon against cyberattacks."[184]

During early 2016, President Barack Obama, while announcing his new cyber budget provisions and cybersecurity initiatives, stated:

> My budget includes more than $19 billion for cybersecurity, which is up by more than one-third. And with this plan, we intend to modernize federal IT by replacing and retiring outdated systems that are vulnerable to attack… one of the biggest gaps between the public

---

[183] *Cyber Operations: Improving the Military Cyber Security Posture in an Uncertain Threat Environment: Hearing Before the Subcomm. on Emerging Threats and Capabilities of the H. Comm. on Armed Services,* 114th Cong. 48-49 (2015), https://fas.org/irp/congress/2015_hr/cyberops.pdf (last visited Mar. 25, 2015) (statement of Admiral Michael S. Rogers, Commander, U.S. Cyber Command and Director, National Security Agency).

[184] *See* Stern, *supra* note 122, at 67.

> sector and the private sector is in our IT space, and it makes everybody's information vulnerable. Our Social Security system still runs on a Cobalt platform that dates back to the '60s. Our IRS systems are archaic… If we're going to really secure those in a serious way, then we need to upgrade them . . .[185]

More Lessons from History

Jason Healey is a former Director of Cyber Policy during the Obama Administration and cautions that "[c]yber history has been forgotten, ignored as irrelevant, or intentionally falsified . . . [while] the issues faced today are largely reflected in, or are exactly the same as, those faced by the previous generation."[186] Today, recruiting skilled talent to defend against cyber attack remains a challenge.[187] However, as Mr. Healey observes about cyber defenders,

> As each new wave of entrants, every five years or so, feels that they are the pioneers. Since they are not taught any history of their field, many accordingly fail to distinguish between what is actually new versus what is just new to them. In addition, cyberspace not only has many characteristics which are non-intuitive to (older) policymakers, but it seems to be forever changing… Admittedly, the field is still emerging rapidly, and we are at the beginning of the 'cyber age.' But that is no reason to ignore the useful lessons of its current history.[188]

---

[185] *Remarks by the President Obama on* New Cybersecurity Initiatives (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/remarks-president-new-cybersecurity-initiatives (last viewed Apr. 13, 2016); *see also President Obama*, *Protecting U.S. Innovation from Cyberthreats,* WALL ST. J. (Feb. 9, 2016).

[186] JASON HEALEY, A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 14 (Jason Healey and Karl Grindal eds., Cyber Conflict Studies Assn. 2013).

[187] *See* Steve Morgan, *One Million Cyber Job Openings In 2016,* FORBES (Jan. 2, 2016).

[188] HEALEY, *supra* note 186, at 16.

For perspective and insight as to vulnerability causation, let us now harken back almost seventy years to findings from the Joint Committee on the Investigation of the Pearl Harbor Attack as they point to "supervisory, administrative, and organizational deficiencies which existed in our Military and Naval establishments in the days before Pearl Harbor."[189] After careful consideration of evidence produced during its investigation, the Joint Committee produced a series of principles "for the reason that, by their self-evident simplicity, it is difficult to believe they were ignored. . . . [And] in the earnest hope that something constructive may be accomplished that will aid our national defense and preclude a repetition of the disaster of December 7, 1941."[190] As our strategy evolves to detect, mitigate, and fight cyberattacks, reflection upon these principles, and how, if at all, they may differ in today's rapidly changing technological environment, may prove helpful. The principles are as follows:

> 1. Operational and intelligence work requires centralization of authority and clear-cut allocation of responsibility.
>
> 2. Supervisory officials cannot safely take anything for granted in the alerting of subordinates.
>
> 3. Any doubt as to whether outposts should be given information should always be resolved in favor of supplying the information.
>
> 4. The delegation of authority or the issuance of orders entails the duty of inspection to determine that the official mandate is properly exercised.
>
> 5. The implementation of official orders must be followed with closest supervision.
>
> 6. The maintenance of alertness to responsibility must be insured through repetition.

---

[189] S. Rep. No. 79-244 at 253, Investigation of the Pearl Harbor Attack: Report of the Joint Committee on the Investigation of the Pearl Harbor Attack (1946).

[190] *Id.* at 254.

7. Complacency and procrastination are out of place where sudden and decisive action are of the essence.

8. The coordination and proper evaluation of intelligence in times of stress must be insured by continuity of service and centralization of responsibility in competent officials.

9. The unapproachable or superior attitude of officials is fatal. There should never be any hesitancy in asking for clarification of instructions or in seeking advice on matters that are in doubt.

10. There is no substitute for imagination and resourcefulness on the part of supervisory and intelligence officials.

11. Communications must be characterized by clarity, forthrightness, and appropriateness.

12. There is great danger in careless paraphrase of information received and every effort should be made to insure that the paraphrased material reflects the true meaning of the original.

13. Procedures must be sufficiently flexible to meet the exigencies of unusual situations.

14. Restrictions of highly confidential information to a minimum number of officials, while often necessary, should not be carried to the point of prejudicing the work of the organization.

15. There is great danger of being blinded by the self-evident.

16. Officials should at all times give subordinates the benefit of significant information.

17. An official who neglects to familiarize himself in detail with his organization should forfeit his responsibility.

18. Failure can be avoided in the long run only by preparation for any eventuality.

19. Officials, on a personal basis, should never countermand an official instruction.

20. Personal or official jealousy will wreck any organization.

21. Personal friendship, without more, should never be accepted in lieu of liaison or confused therewith where the latter is necessary to the proper functioning of two or more agencies.

22. No considerations should be permitted as an excuse for failure to perform a fundamental task.

23. Superiors must at all times keep their subordinates adequately informed and, conversely, subordinates should keep their superiors informed.

24. The administrative organization of any establishment must be designed to locate failures and to assess responsibility.

25. In a well-balanced organization there is close correlation of responsibility and authority.[191]

A major difference between the environment surrounding Pearl Harbor and the cyber domain, according to Harvard National Security Fellow Steven Anderson, "is the fact that the military owns less than 15% of the cyberspace environment . . . so integration between the military/public/private sectors is absolutely critical if the nation is going to prevent an event as depicted earlier in this paper . . . let alone how to respond if/when it does occur."[192]

VII. CONCLUSION

"Intelligence is all about the future and is designed to enable action in the face of continuing doubt."

Gen. Michael V. Hayden
Former Director of the National Security Agency and CIA[193]

---

[191] S. Rep. No. 79-244 at 253-262.

[192] E-mail from Steve "Canyon" Anderson, Lt Col, USAF, National Security Fellow, Harvard Kennedy School, to Lawrence J. Trautman (Mar. 28, 2016, 16:03 CST) (on file with author).

[193] HAYDEN, *supra* note 47, at 233.

With the power to wreak havoc on global economic and political stability, cyber issues remain likely the greatest single threat to modern civilization. Now, just as in the days and weeks immediately preceding the 1941 attack against the United States at Pearl Harbor, all the necessary warning signs are there. Enemies have probed and fully mapped the data systems of America's important corporations and institutions. The future of the United States, represented by its intellectual property, has systematically been stolen by its adversaries. Initial sounding of the alarm, "the hackers are coming; the hackers are coming" may have already faded from deaf ears. However, beware, the hackers are here! The hackers are here!