Origins of Cyberwarfare: How the Internet got Weaponized

Ada Peter and Ujunwa Ohakpougwu
Communications Department, Covenant University, Nigeria

ada.peter@covenantuniversity.edu.ng;
ado909@g.harvard.edu
Ujunwa.ohakpougwu@stu.cu.edu.ng

Abstract: Cyberspace was until last decade and half a perfect additional intelligence gathering tool. Within a phase of time during the spread of the world wide web, the cyberspace expanded outside the boundaries of intelligence gathering to a perfect weapon in the hands of both state and non-state actors for destabilizing or devastating the state of critical infrastructures of perceived enemy or competitors. In the heart of the storm, Social Scientists have either focused on extensive definitions and clarifications of cyberwar, others are fixated on explaining the various emerging dangers of cyber weapons on society, like the consequences of weaponizing the cyberspace against a nation's power grid, nuclear command, and control systems, neutralizing a petrochemical plant, paralyzing a government's health care or governance structure and possibilities of manipulating elections. But few, if any have considered the question which is central to this paper: How did the cyberspace evolve from an intelligence tool to a cyberweapon against critical infrastructures? The obvious answer is that the magnified global access and use of networked systems provided the perfect battle space for deploying cyberweapons. The preceding explanation is essentially correct, but it is entirely lacking in detail explaining how cyberspace became weaponized? Under what conditions was cyberspace purely an intelligence tool. Under what conditions is cyberspace weaponized? This research incorporates these and other questions into a framework through the means of a model designed to aid understanding of how the cyberspace evolve from an intelligence tool to a destructive weapon targeted at critical infrastructures. Primary sources include relatively untapped 107 Congress Laws on Cyber related legislations. From the 105th congress to the current 116th congress, 1, 177 legislations have been introduced on cyber or cyber related issues. Other primary sources include White House fact sheets, statements, press releases, President Trump's 2018 National Cyber Security Strategies, President Obama's 2016 Cyber Security National Action Plan, and cyber related executive orders, statements, and press releases from President Johnson of the last 5 US administrations.

Keywords: Cyberwar, cyberweapons, cyberspace, cyberwarfare, U.S legislations, National Cyber Security Strategies

1. Introduction

Cyberspace was until the 21st century, an additional intelligence-gathering and communication tool. As an intelligence tool, state actors collected secret or open information via covert or overt digital activities. The secret information ranged from U.S. data about the intentions and capabilities of other nations to U.S. understanding of the level of data other nations have about U.S. surreptitious capabilities and intentions. The covert activities seemed like inter-national hide and seek games, guided by self and globally initiated rules. The massive leak of NSA documents in 2005 detailing U.S. surveillance programs, accessing internet company data, eavesdropping, and tapping fiber optic cable explains how nations collected information through covert digital activities (Popovich and Chen 2013).

While it is arguable that intelligence gathering through cyber means was a weapon that provided undue advantage over allies and adversaries, at the time however intelligence gathering through cyber means lacked the sole capability of wreaking havoc without successive actions and decisions. Intelligence gathering through cyber means was by itself harmless unless used as the basis for decisions and actions that may be destructive.

However, beginning February 1990, when the era of military involvement in the operation of the internet ended, and ARPANET decommissioned, the network grew faster, access and use of the world wide web spread like an unending spider web, and the cyberspace expanded outside the boundaries of intelligence gathering to a perfect weapon in the hands of both state and non-state actors who destabilize or devastate critical infrastructures of perceived enemy or competitors. These state and non-state actors used the cyber weapon to incapacitate an adversary's national critical infrastructure, frustrate it, slow it, undermine its institutions, and leave its citizens angry or confused (Sanger 2018). Examples include the 2022 disruption of US gas pipelines, Russia's alleged use of fake social media campaigns to interfere in U.S. 2016 presidential election; the late November 2014 North Korean attack on Sony Pictures in connection to the planned release of the poorly reviewed movie *the interview;* the 2010 American *Stuxnet* attack on Iran and North Korea's weapons program*,* the Chinese decades-long espionage of U.S. trade secrets, and 2007 Russian attack on many of Estonian government departments, political parties, media organizations, and companies.

At the heart of the cyber weaponization storm, social scientists have focused on extensive definitions and clarifications of cyber warfare, what it means, what it entails, and whether threats can deter, or defense can

mitigate its effects. These studies often attempt to explain the various emerging dangers of cyber weapons on society, like the consequences of weaponizing the cyberspace against a nation's power grid, nuclear command, and control systems, neutralizing a petrochemical plant, paralyzing a government's health care or governance structure and possibilities of manipulating elections (Healey 2013).

But few, if any, have considered the question central to the current research: How did the cyberspace evolve from an intelligence tool to a cyber weapon against critical infrastructures? The obvious answer is that the magnified global access and use of networked systems provided the perfect battle space for deploying cyberweapons. As Abbate puts it, the worldwide system called the Internet played a significant role in developing and popularizing network technology, which placed computers at the center of a new communications medium (Abbate. 1999). Between the late 1960s and the 1990s, the Internet grew from a single experimental network serving a dozen sites in the United States to a globe-spanning system linking millions of computers. It brought innovative data communications techniques into the mainstream of networking (Abbate 1999). The preceding explanation is essentially correct, but entirely lacks details explaining how cyberspace became weaponized. Under what conditions is cyberspace purely an intelligence tool? Under what conditions is cyberspace weaponized? When does the change happen?

What aspects of cyberspace do government budget and money target? What aspects of cyberspace do trainings target? What government agencies are responsible for what or to do what? By what growing government legislative efforts do cyber dependent societies sustain resilience of Critical Infrastructure? When and why do cyber policies in the U.S. change to respond to the emergence of cyberspace as a weapon? Under what conditions do these policy changes occur? What modifications do the U.S. Department of Defense (DoD) policies and Cybersecurity Executive Orders seek to protect critical infrastructure from cyber weapons?

Hence the objective of the research is to outline a model that will aid the understanding of how the cyberspace evolves from an intelligence tool to a destructive weapon targeted at critical infrastructures. Critical infrastructures as operationalized within the Executive Order on *Improving Critical Infrastructure Cybersecurity*, include systems and assets, whether 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 or safety, or any combination of those matters.

The model serves as preliminary and a heuristic device useful in facilitating a conversation on relatively important but ignored details of cyberspace. More broadly, the outcome of the research adds to the literature useful for subsequent studies targeting theory building about state shifts in the use of cyberspace. Dissecting how the cyberspace evolved to a weapon may also provide useful insight into leverage points that are useful for cyber policymaking process, where small change could lead to a large shift in behaviour

2. Research Methods

The work adopts the case study approach. During the exploratory phase, we discovered that the first mention of the closest cyber-related word ‘internet’ in U.S. legislation was in the S.1001. bill 1987, focusing on promoting and providing increased access. The next two mentions of the Internet occurred three years after in the House and Senate of the 102nd Congress (1991 – 1992). Thus, while the model will attempt to capture and classify cyber intelligence activities prior to 1994, the primary sources for the research will include relatively untapped 107 Congress Laws on Cyber related legislations and cyber-related executive orders from 1992 to 2022 when a Russian-speaking group of hackers knocked multiple US airport websites offline (Wallace et.al 2022).

Congress Laws on Cyber related legislations and cyber-related executive orders within these three decades will show exactly when and how the aims of the legislations shifted from promoting the internet and improving access to protecting against cyberattacks.

The researcher extracted the laws from Congress.gov, the official website for U.S. federal legislative information. The site provides access to accurate, timely, and complete legislative information for Members of Congress, statutory agencies, and the public. It is presented by the Library of Congress (L.O.C.) using data from the Office of the Clerk of the U.S. House of Representatives, the Office of the Secretary of the Senate, the Government Publishing Office, Congressional Budget Office, and the L.O.C.'s Congressional Research Service (Congress.gov 2012). The Congress.gov search with the keyword “Cyber” returned 1225 legislation, 746 originated from the House and 479 from the Senate, of the 1225, only 107 were converted to laws. See figure 1 for the timeline of U.S. cyber-related bills passed into law.

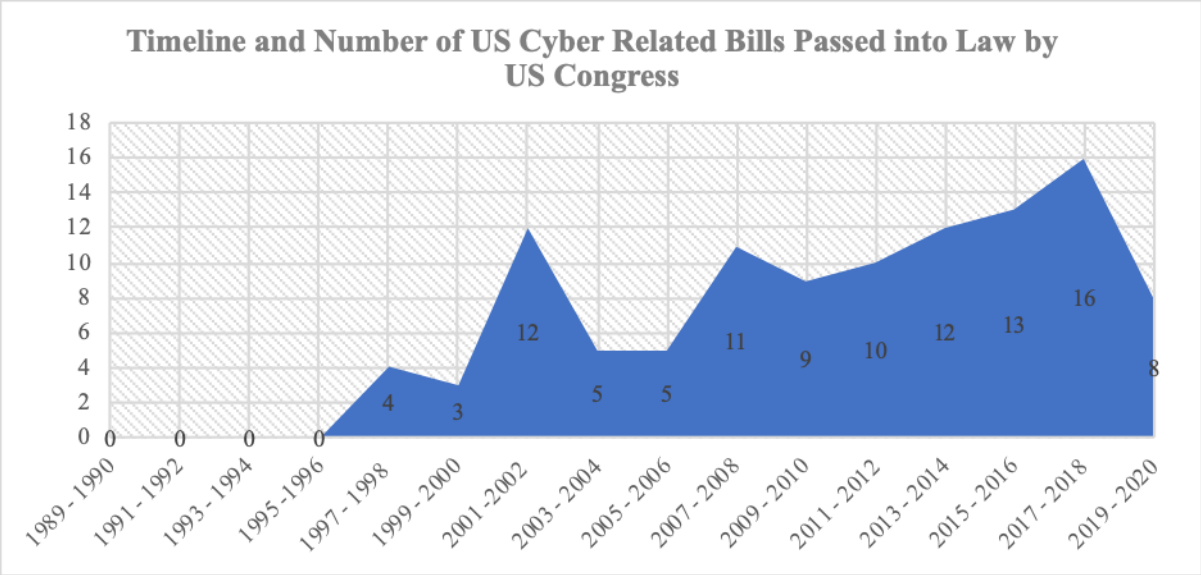

Figure 1 consists of U.S. cyber-related bills passed into law by U.S. congress between 1997 (105th Congress) and 2020 (116th Congress). I classified the laws according to the rate of bills passed into law by respective congresses. For instance, the year 1997 – 1998 in figure 2 indicates that the 105th Congress passed four cyber-related bills into law, while the 115th Congress between 2017 -2018 passed 16 cyber-related bills into laws. It is essential to highlight that the numbers in figure 2 represent cyber-related bills that became laws. I did not include cyber-related bills introduced to Congress, considered by committees, floors, or passed by one or both chambers in the study.

Figure 1: Timeline and Number of U.S. Cyber Related Bills Passed into Law by U.S. Congress

The study opted for legislation passed into law since these are rules that the United States accepts and recognizes as regulating stakeholders' actions, especially citizens and inhabitants. Using laws does not mean that the content of the U.S. Congress laws used for the study captures all the actions that transpired in all three phases among citizens, nor does it mean that these mandated laws are the only factors responsible for the cyber weaponization as it is today. Instead, the study opted for U.S. congress laws since it can reveal nationally binding and mandated actions about the existing cyber developments in the United States.

The other group of primary sources include 14 executive orders from the Clinton to the Trump administration. The reason is that executive orders often have much the same power as a law. Executive orders, a type of executive action, play a significant role in the U.S. President's ability to enforce the laws of the United States.

3. Research Limitations

The model is strictly based on the US data. The model does not represent the processes or interpretations of US cyber strength and vulnerabilities by external allies, partners, or enemies. It is only a representation of the picture of the processes and interpretations of cyber strength, vulnerabilities and weaponization in the United States. Moreover, the findings of the study may not represent the cyber weaponization processes in other developed and cyber reliant economies.

4. Preliminary Model

From the preliminary inductive approach to content analysis of the primary data, the goals, targets, and aims of the bills appeared in patterns, which I generalized into a model that describes how cyberspace evolves from an intelligence tool to a cyber weapon targeted at protecting and destabilizing critical infrastructures. Three overlapping phases of intra-country processes constitute the proposed model. See figure 2

Each phase has core tenets that defines and makes the proposition of the model testable and falsifiable. For instance, the core tenets and indicators of the cyber independent phase are legislations and theme dominantly promoting improved access, spread, diffusion of innovation, intelligence collection dominates. The legislation and funding barely target protection and security of cyberspace from adversaries. More so less than a third of the critical infrastructure sectors are dependent on cyber to function. Appropriations are implicit about the available funding specific to cyber.

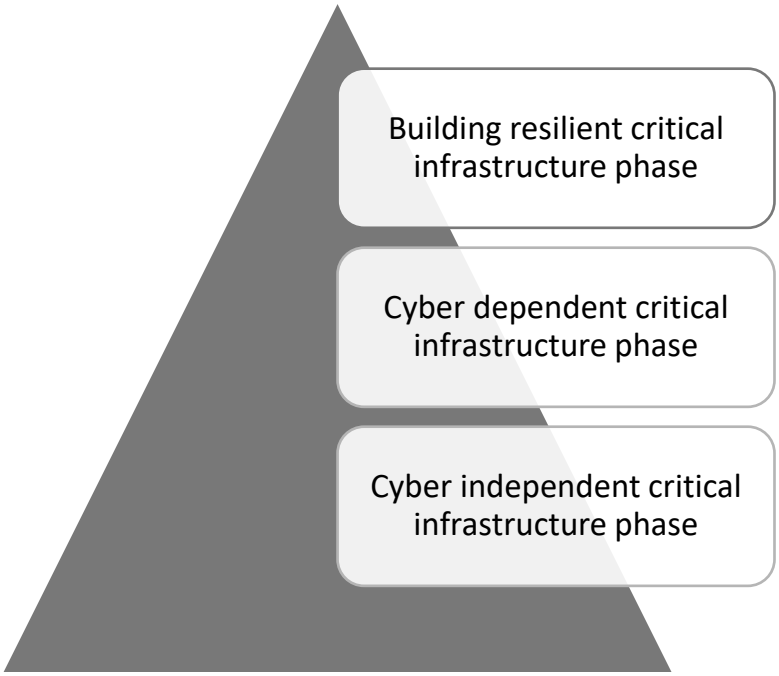

Figure 2: Preliminary model of how cyberspace evolves into piercing weapons

The next phase is dominated by legislation that prioritize protection over access, spread, diffusion of innovation, both in terms of budgetary allocations and legislation passed, including legislation to prepare human and mechanical capacities against potential attacks

More than a third of the critical infrastructure sectors are dependent on cyber to function and there is a growing awareness and sensitization of different stakeholders about the remarkable impact of an attack targeted at cyber dependent critical infrastructures. Appropriations are barely explicit about the available funding specific to cyber.

The last phase legislation prioritizes and drives institutionalization of security, norms, ethics in cyberspace because at this point nearly all 16 critical infrastructure sectors depend on cyber to function. More than half of the 16 critical infrastructure sectors experienced noteworthy annual cyber-attacks. In the phase, the risk and vulnerability of cyber-attacks increases. The demand to close any legislative gaps that may expose U.S. infrastructures to grave disruptions and losses also increases. Appropriations are explicit about the available funding specific to cyber. Cyber still serves as a communication and an intelligence-gathering tool for government but human capabilities are prepared for retaliatory and offensive attacks; numerable critical infrastructure sector-specific agencies exist at both federal and state levels; Risk and vulnerability to cyber-attacks spreads into every sector.

A remarkable insight is that the legislative priorities and themes of a former phase drips into the latter phase but not vice versa. For instance, the legislative priorities and themes of the cyber independent phase trickles into the cyber dependent phase and the legislative drives of both phases' trickles into the building resilient critical infrastructure phases but not the reverse. It means that there can be few legislative themes focusing on improved access in the building resilient phase but there can't be themes for institutionalization of security, norms, ethics in cyberspace in the cyber independent critical infrastructure phase. The flowing paragraphs provide more explanation and preliminary evidence about each phase.

The cyber independent critical infrastructure phase: This is the pre-weaponization stage. During this phase, cyber served as a communication and an intelligence gathering tool for government**.** The first photo reconnaissance satellite that will aid military observation of a region to locate an enemy or to ascertain its strategic features was launched in 1962 (Federation of American Scientist 1996). Though these technical collection efforts had been ongoing for several years in both C.I.A. and the Air Force, they were formally consolidated, pursuant to a national security directive, in 1961 within the National Reconnaissance Office (NRO).

During the cyber independent critical infrastructure phase, cyber related laws were also mostly federal laws not State laws targeted at building cyber dependent infrastructures. The focus of U.S. legislations was on computer

fraud and deterring unauthorized access to computers. The dominant legislation at the time was the United States Computer Fraud and Abuse Act which was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030) (Doyle 2014). According to the law, access to a computer without authorization or exceeded authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation (Computer Fraud Act 2006). The reason why the U.S. legislations focused more on deterring unauthorized access to information and communication technology and fraud and related activity in connection with computers is that before the Internet became a globe-spanning system linking millions of computers from the late 1990s, the network technology was only deployed as experimental networks serving a dozen sites in the United.

The cyber independent critical infrastructure was also marked by efforts of the U.S. legislative to provide network access to the Internet to an increasing number of sectors. At the early stage of the phase, the legislative attention to the need for network access for more sectors appeared weak. Any bill proposing more access was more likely to wind-up at the introductory stage of the legislative process. For instance, the first mention of the closest cyber-related word 'internet' in U.S. legislation was in the S.1001. bill 1987

The S.1001. was a bill to amend title IV of the Social Security Act to improve the performance of States in establishing the paternity of children, assuring the adequacy of child support award amounts, and enforcing child support awards. The bill which was sponsored Senator Bill Bradley in the 100th Congress (1987 -1988) was read twice and referred to the Committee on Finance, where it died. The mention of the Internet in the bill reads

> *"Directs the Secretary to enter into an agreement with the Secretary of Labor to provide the Parent Locator Service with prompt access to the INTERNET system which tracks interstate unemployment insurance claims of the State employment security agencies and the Labor Department."(*S.1001 1998)

The next two mentions of the Internet occurred three years after in the House and Senate of the 102nd Congress (1991 – 1992) and again these bills did not exceed the introduction status of legislation, meaning that when the bill was referred to the Senate Committee on Commerce and the House Subcommittee on Science respectively, these committees did not act on the bills, an equivalent of killing it. The initial was in the HR 5759: *Information Infrastructure and Technology Act of 1992*, sponsored by Rep. George Brown, and the next was in S. 2937: *Information Infrastructure and Technology Act of 1992*, sponsored by Sen. Albert Gore.

Though these Information Infrastructure and Technology bills did not make it past the committees and subcommittees, Senator Gore and Rep. Brown's legislative attempts indicate that the cyberspace, a budding information infrastructure that required more funding to deploy more technologies into other critical infrastructures in various sectors, was in 1991 merely in its pre-smart phase in the U.S.

Towards the end of the cyber independent critical infrastructure phase, the first-ever cyberattack, the Morris worm, occurred by mistake. Robert Tappan Morris, in 1988 developed a program to assess the size of the Internet. The program would crawl the web, install itself on other computers, and then count how many copies it made. Once tallied, the results were supposed to indicate the number of computers connected to the Internet (Climer 2018). Instead of following the desired command in computers where it was installed, the worm infected and incapacitated computers until they finally crashed.

Structuring cyber reliant critical infrastructure phase: Also known as the weaponization phase. Here, more than one third of 16 critical infrastructure sectors are dependent on cyber to function; In October 1997, the President Bill Clinton's Commission on Critical Infrastructure Protection issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures. According to the report, the president's intent was that the United States will take all necessary measures to eliminate any significant vulnerability to both physical swiftly and cyber-attacks on our critical infrastructures, including especially our cyber systems. The cyber dependent critical infrastructures were telecommunications, banking and finance, energy, transportation, and essential government services (The White House 1998).

The United States desperately reckoned with existing human and infrastructure gaps in the prevention and response capabilities of state and local law enforcement agencies to cyberattacks. Federal law inspired government agencies to start training and acquiring equipment that will assist in the prevention and quick response to cyber-attacks. Congress began to introduce and pass legislation to prepare human and mechanical capacities against potential attacks. The appropriation acts captured expenditures for the protection of

cyberinfrastructures; the U.S. government embraced the necessity to set money aside for the protection of cyberinfrastructure.

It was until this phase that the political will to cover and refund "any cost" incurred by all federal government agencies if the cost was associated with preparing and improving the competencies of human and mechanical competencies to respond and or prevent cyber-attacks. Appropriation Acts or bills explicitly captured preventing cyberspace dangers as worthy of national goal and attention. On May 22, same year, 1998, the Clinton administration issued the Presidential Decision Directive 63 (The White House 1998).

The PDD-63 outlined the increased reliance on cyberinfrastructure by public and private enterprises, and the strong need for collaboration to improve the security of this infrastructure. The directive marked the first White House effort to address vulnerabilities from the United States dependence on cyberspace and established a framework to encourage information sharing and collaboration among various sectors (Spaulding 2013)

By the 105th Congress (1997 – 1998), the term 'cyber' was first used in U.S. bills. From a congress that passed no bill citing cyber to a congress that introduced six legislations, that passed both chambers, and four became laws. The four laws targeted were appropriations for the Department of Defense in the fiscal year ending September 30, 1999. Other purposes include reimbursing departments and agencies of the Federal Government for any costs incurred in connection with "providing training and related equipment for the chemical, biological, nuclear, and cyber-attack prevention and response capabilities to State and local law enforcement agencies" (Rogers 1997).

Beginning November 1998, the federal U.S. annual legislation passed into law on cyberinfrastructure protection never decreased below three (See figure 2). The 111th Congress between 2009 and 2010, considered 93 legislations, the highest of the immediate past five congresses before 2009. Ten of these passed both chambers and nine became laws.

The weaponization phase is also marked by growing awareness and sensitization of different stakeholders about the remarkable impact of an attack targeted at cyber dependent critical infrastructures. But evidence of cyber-attacks on these infrastructures were still absent during this phase indicating that the in-country cyberspace is still a budding attractive war space for known and unknown state enemies. The risks, threats and vulnerability to cyber-attacks were not as palpable as it appeared in the weaponized phase. In a 2001 congressionally required annual report on the Status of Federal Critical Infrastructure Protection Activities, the National coordinator of Infrastructure Assurance Council, Richard Clarke, who warned of a possible "electronic Pearl Harbor, highlighted to the President, heads of departments and agencies in pursuant of the implementation of PDD-63, the potential threats and vulnerabilities of cyber dependent infrastructures. Actual cases of cyberattacks were absent from the report.

To foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the Former U.S. President, Bill Clinton, in PDD-63 emphasized that

> *"The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations."* (The White House 1998).

The signs and possibilities of cyberspace becoming the fifth dimension of warfare that could complement the four U.S. standard dimensions: land, sea, air, and space were apparent.

Before the end of former President Clinton tenure, he writes in one executive order that, "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and government continuity. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radiofrequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats") (Clinton, 1996)

Building resilient critical infrastructure phase: Classified as the third phase, nearly all 16 critical infrastructure sectors depend on cyber to function. More than half of the 16 critical infrastructure sectors experienced noteworthy annual cyber-attacks. Numerous domestic instances, cases or opportunities that stimulate a sense of urgency for proposed cyber-related bills abound. In a survey of 24 federal agencies, G.A.O., the United States Government Accountability Office, reported that between 2006 and 2015, the number of cyberattacks climbed 1,300 percent — from 5,500 to over 77,000 a year (GAO 2016). Statista, a statistics portal with directly accessible data for 170 industries and 50 countries, also reported that data breaches and records exposed in the United States between 2005 and the first half of 2018 number in the millions (Statista 2018). These data breaches in the United States amounted to 668, with over 22 million records exposed.

Between the 112th and 116th congresses in 2020, 876 more legislations were introduced by different lawmakers. These increases suggest U.S. shifts from a nation-building preliminary infrastructure and seeking to provide access to a nation embracing the growing and exponential sense of urgency for the protection of U.S. cyberspace and cyber dependent critical infrastructures from attacks that threaten national security.

In the phase, the risk and vulnerability of cyber-attacks increases, so the demand to close any legislative gaps that may expose U.S. infrastructures to grave disruptions and losses. Congress or tiers of government laws targeted improving the resilience of cyber dependent infrastructures, increasing human capacities and competencies, and connecting more critical infrastructure to cyber-enabled networks; Congress or all tiers of government laws targeted protection of existing cyberinfrastructure; For instance, as soon as the American Recovery and Reinvestment Act of 2009 provided the U.S. Department of Energy with $4.5 billion to modernize the electric power grid (SmartGridGov 2020), research funds for capacity building were captured in the appropriation Acts. One of the sample appropriations Acts, the **[**H.R. 3183] Energy and Water Development and Related Agencies Appropriations Act, 2010, highlights these points

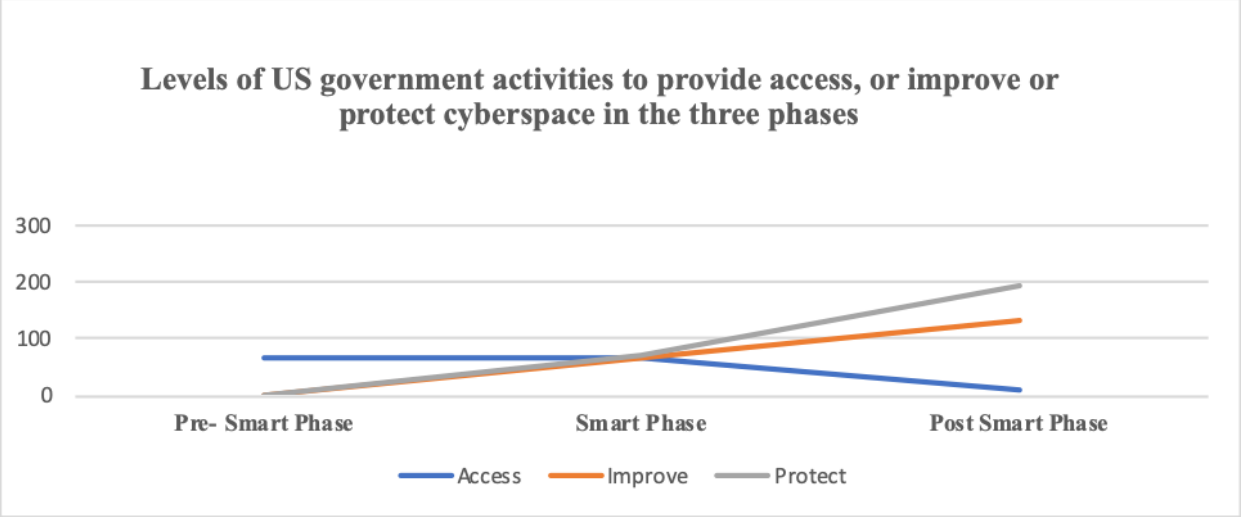

Figure two illustrates the government's attention to access, the need to improve and protect critical infrastructures during each phase.

During the third phase, the U.S. cyberspace became an attractive war space for known and unknown state enemies; even though cyber still serves as a communication and an intelligence gathering tool for the U.S. government, the U.S. is making budgetary allowance to increase the of rate human capabilities prepared for retaliatory or offensive attacks; There are numerous critical infrastructure sector specific agencies at both federal and state and community levels. Appropriation is explicit about the available funding specific to cyber. (See figure 3).

Each Secretary of a military department shall

'The defense agency and funds focus on deploying human capacity to reduce the risk of cybersecurity threats posed by quantum information science technology. Cyberspace is acknowledged as war space

Section. 220. on the modification of defense quantum information science and technology research and development program authorizes the department of defense to select for the Detachment, and make efforts to retain, members of the reserve components who possess relevant private-sector experience in the fields of business, acquisition, intelligence, engineering, technology transfer, science, mathematics, program

management, logistics, cybersecurity, or such other fields as determined by the Under Secretary of Defense for Research and Engineering (National Authorization Act, 2020)

Besides Section 361 subsection 1 acknowledges the cyberspace as a war space description of each readiness problem or deficiency that affects the ground, sea, air, space, cyber, or special operations forces, and any other area determined appropriate by the Secretary of Defense (National Authorization Act, 2020).

In the third phase, citizens are most conscious, prepared or trained about of the risks of the smart county**;** most relevant national tertiary institutions have technical competencies and evidence of improved cyber technologies; all 16 critical infrastructure sectors depend on cyber; any cyber-attack on critical infrastructure that will inflict remarkable effects on the affected critical infrastructure sector; Congress or tiers of government laws are targeted at improving the protection of cyber dependent infrastructures, increasing human capacities and competencies for the protection of cyberinfrastructures, and increasing the resilience of cyber dependent critical infrastructure; Congress or all tiers of government laws are targeted at protection of existing cyberinfrastructure; in-country cyberspace is a full-blown attractive war space for known and unknown state enemies; cyber still serves as a communication and an intelligence-gathering tool for government but human capabilities are prepared for retaliatory and offensive attacks; numerable critical infrastructure sector-specific agencies exists at both federal and state levels; Risk and vulnerability to cyber-attacks spreads into every sector.

Most critical infrastructures are interconnected, and maximum efficiency cyber and according to the Cybersecurity and Infrastructure Security Agency (CISA 2020), 16 cyber dependent critical infrastructure sectors exist today. These sectors include Chemical sector, Commercial Facilities, Communications sector, Critical Manufacturing sector, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Sector, Information Technology, Nuclear Reactors, Material and Waste, Transportation Systems, Water and Wastewater Sectors.

5. Preliminary Conclusions

The preliminary analysis indicates that the cyber shifts from an intelligence tool to a weapon strode through the following phases in government legislations: the cyber independent critical infrastructure phase, structuring cyber reliant critical infrastructure phase, and building resilient critical infrastructure phase. The model is preliminary and a heuristic device useful in facilitating a conversation on relatively important but ignored details of cyberspace. More broadly, the preliminary study provides good descriptions that will be useful for theory building in my thesis about state shifts in the use of cyberspace.

References

Abbate, Janet. 1999. *Inventing the Internet.* Cambridge: M.I.T. Press.

Barrett, Brian. "D.O.J. Charges North Korea Hacker for Sony, WannaCry, and More (Links to an external site.)." *Wired,* September 6 2018.

Bennett, Andrew and Jeffry T. Checkel. Process Tracing: From Metaphor to Analytic Tool. (2015) Cambridge: Cambridge University Press. ISBN: 978-1-107-68637-3

Charles Doyle (2014) Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws . Congressional Research Service https://fas.org/sgp/crs/misc/RS20830.pdf;

Clapper, James. "Cyber Deterrence Policy." C-SPAN.org. May 11, 2017. Accessed December 2, 2018. https://www.c-span.org/video/?428339-1/intel-chiefs-testify-us-cyber-defense-strategy.

Computer Fraud and Abuse Act (18 USC 1030) https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

Computer Fraud and Abuse Act (18 USC 1030) https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

Cybersecurity and Infrastructure Security Agency (CISA). 2020. *CRITICAL INFRASTRUCTURE SECTORS.* March 24. Accessed April 24, 2020. https://www.cisa.gov/critical-infrastructure-sectors.

Dey I. (1993) Qualitative Data Analysis. A User-Friendly Guide for Social Scientists. Routledge, London.

Federation of American Scienctist (February 1996). The Evolution of the U.S. Intelligence Community-An Historical Overview https://fas.org/irp/offdocs/int022.html

George, & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Greg Wallace, Sean Lyngaas, Pete Muntean and Michelle Watson, CNN (Oct 10, 2022) https://www.cnn.com/2022/10/10/us/airport-websites-russia-hackers/index.html

Jamieson, Kathleen. *Cyberwar - How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*. New York: Oxford University Press, 2018. https://global.oup.com/academic/product/cyberwar-9780190915810?cc=us&lang=en&#

King, Gary, Keohane, Robert O. and Verba, Sidney. Designing Social Inquiry: Scientific Inference in Qualitative Research, Princeton University Press, 1994.

Krebs, Brian. "F.B.I.: North Korea to Blame for Sony Hack. (Links to an external site.) (Links to an external site.)"December 14 2014.

Libicki, Martin. *Cyber deterrence and cyberwar*. Santa Monica, CA: RAND Corporation, 2009. https://www.rand.org/pubs/monographs/MG877.html.

National Authorization Act, 2020, S. 1790, 116th Cong. (2019) Supporting Veterans in STEM Careers Act, Pub. L. 116–115, 134 STAT. 107 (2020)

National Authorization Act, 2020, S. 1790, 116th Cong. (2019) Supporting Veterans in STEM Careers Act, Pub. L, 116–115, 134 STAT. 107 (2020)

Peter, Ada S. 2017. "Cyber Resilience Preparedness of Africa's Africa's Top-12 Emerging Economies." International Journal of Critical Infrastructure Protection 17 (June): 49–59. https://doi.org/10.1016/J.IJCIP.2017.03.002.

Research, SmartGridgov - *Advanced Grid - Initiatives that catalyze the industry to modernize the grid.* Accessed April 24, 2020. https://www.smartgrid.gov/.

Research, SmartGridgov - Advanced Grid - Initiatives that catalyze the industry to modernize the grid 2020)

S.1001 - A bill to amend title IV of the Social Security Act to improve the performance of States in establishing the paternity of children, assuring the adequacy of child support award amounts, and enforcing child support awards.100th Congress (1987-1988)

Sanger, David. 2018. *The Perfect Weapon.* Penguin Random House.

Schmitt, Michael. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum." *Harvard National Security Journal* 8 (February 17): 281-82.

Schneier, Bruce. "Lessons from the Sony Hack (Links to an external site.) (Links to an external site.)." *Wall Street Journal,* December 19 2014.

Siobhan, Climer (2018). History Of Cyber Attacks From The Morris Worm To Exactis https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/

Suzanne Spaulding (2013) The Atlantic Council. *15th Anniversary of PDD-63: History of Cyber Critical Infrastructure Protection.* https://www.atlanticcouncil.org/commentary/event-recap/15th-anniversary-of-pdd63-history-of-cyber-critical-infrastructure-protection/

Tetlock, Philip E. and Aaron Belkin (1996). Counterfactual Thought Experiments in World Politics. Princeton: Princeton University Press. ISBN: 0-691-02791-9.

The Statistics Portal," Statista, , accessed December 17, 2018, https://www.statista.com/aboutus/.

The White House (1998). The Congressional Research Service. *Presidential Decision Directive/Nsc-63* https://fas.org/irp/offdocs/pdd-63.htm

The White House (1998). The Congressional Research Service. *Presidential Decision Directive/Nsc-63* https://fas.org/irp/offdocs/pdd/pdd-63.htm

The White House (1998). The Congressional Research Service. *Presidential Decision Directive/Nsc-63* https://fas.org/irp/offdocs/pdd-63.htm

United States Government Accountability Office, Information Security, FDIC Needs to Improve Controls over Financial Systems and Information: Report to the Chairman, Federal Deposit Insurance Corporation (United States, 2016).

United States Government Accountability Office. *Information Security, FDIC Needs to Improve Controls over Financial Systems and Information: Report to the Chairman, Federal Deposit Insurance Corporation*. United States, 2016.

United States Government. White House Office of Trade and Manufacturing Policy. White House. *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*. Washington: United States Government, 2018. 2-3.

White House, "Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment." *Obama Press Release*, December 29, 2016, https://perma.cc/C83Z-SQSL

William J. Clinton, (1996). Executive Order 13010—Critical Infrastructure Protection. https://www.presidency.ucsb.edu/documents/executive-order-13010-critical-infrastructure-protection