As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(12): 137-143, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0812021
Available online at: http://www.ijmtst.com/vol8issue12.html

Will cyberweapons deter war?

Ishan Mukherjee

Independent researcher, Varanasi, Uttar Pradesh, India

To Cite this Article
Ishan Mukherjee. Will cyberweapons deter war?. International Journal for Modern Trends in Science and Technology 2022, 8(12), pp. 137-143. https://doi.org/10.46501/IJMTST0812021

Article Info
Received: 26 November 2022; Accepted: 25 December 2022; Published: 31 December 2022.

ABSTRACT

The recent surge in the destructiveness of cyberweapons raises the question: will cyberweapons merely be among the most potent weapons in a country's arsenal? Or, will they behave like nuclear weapons do in the present world order: as deterrents against interstate conflict? To answer this question, this paper first clarified exactly what gives nuclear weapons deterring ability. A list of three necessary criteria for conflict-deterring technology was generated: extreme destructiveness, ease of delivery, and resilience against a disarming first strike. Since cyberweapons fulfill these criteria, they can, in principle, deter war. Finally, the challenges to cyber deterrence were evaluated, along with recommendations for policymakers and charitable foundations concerned about international security.

KEYWORDS: *Cybersecurity, Cyberwarfare, Information security, Deterrence theory*

1. INTRODUCTION

The Russian invasion of Ukraine was preceded by a string of cyber-attacks on Ukraine's power grid. Over the years, we have seen cyber-attacks grow in destructiveness, with some comparing the destructiveness of a major cyber strike with that of a nuclear attack [1]. The question arises: will cyberweapons merely be among the most potent weapons in a country's arsenal, or will they behave like nuclear weapons do in the present world order, as deterrents against interstate conflict? To answer this question, we must first clarify what gives nuclear weapons their conflict-deterring ability.

2. WHY DO NUCLEAR WEAPONS DETER WAR?

Nuclear weapons are tools of deterrence not just because they make defeat costly (by being extremely destructive), but because they make victory impossible. This is because a state can use its nuclear weapons even when it is losing, or "on its last legs," in a conventional conflict (in this paper, this property is called the "last-legs usability" of nuclear weapons).

Last-legs usability comes from two factors:

- **Resilience:** Nuclear weapons can deliver enormous explosive force per warhead. So, for a disarming strike to be effective, practically every silo and nuclear submarine would need to be eliminated, which is nearly impossible given the difficulties around detecting submarines [2].
- **Ease of delivery:** Intercontinental ballistic missiles may be launched from trucks and mobile rail-based launchers. Strategic bombers can fly low to evade radar sensors. Submarine-launched missiles can devastate coastal cities [3]. In the pre-nuclear age,

the losing state would usually have lost control over land, air and water, making deadly retaliation impossible. Today, it doesn't matter whose fighters patrol the skies and destroyers skim the seas: even a country on the brink of total annexation can lethally punish its invaders.

We therefore have a set of necessary conditions a weapons technology must fulfill to deter conflict. It must be

- *totally destructive*,
- *resilient*, and
- *easy to deliver*.

In the next section, we'll see how cyberweapons fulfill each of these three criteria.

3. Cyberweapons as Deterrents Against War

A. Destructiveness

The US Department of Defense's Law of War Manual [4] outlines at least three ways in which cyberweapons may cause mass casualties: they may "(1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes." Disrupting train signaling systems or a network of self-driving cars could lead to massive accidents as well. Cyber-attacks on medical devices, such as pacemakers or insulin pumps, could compromise their operation and lead to serious injury or death [5].

All of these are probably limited in scope, however, compared to a cyber-attack on a nation's power grid. A threat assessment by Lloyd's of London, an insurance underwriter, concludes that a cyber-attack on the US power grid could cost over $240 billion in economic losses [6], and substantial loss of life if essential services such as healthcare are disrupted [7]. If a major power outage lasts weeks, the struggle to acquire food and supplies could spiral into rioting and other incidences of violence.

Hacking into air defense systems could allow an attacker to launch a lethal missile strike against an undefended enemy. We saw this play out in 2007, when Israel bombed the al-Kibar nuclear reactor in Syria [8]. To ensure the success of the bombing run by Israel's non-stealthy aircraft, hackers fed Syria's air defense systems a false sky-picture while Israeli fighter jets flew over Syrian territory [9].

Perhaps most concerning of all, a cyberweapon that disables or engineers supervisory control and data acquisition systems (SCADA) controlling the functions of sewer, water treatment and nuclear systems could trigger global nuclear and biological catastrophes [10]. A 2018 study by the Nuclear Threat Initiative [11] found that "[n]uclear weapons and related systems are increasingly vulnerable to sophisticated cyberattacks." Reference [12] offers a deeper look into the issue.

So far, the only known cases in which a cyber operation was involved in the loss of life are state-led assassinations [13]. In 2009, the Kyrgyzstani intelligence agency hacked into the email account of the journalist Gennady Pavlyuk and fabricated a story to lure him out of the country and kill him. The following year, the Israeli intelligence agency Mossad gained information critical to planning Hamas leader Mahmoud al-Mabhouh's assassination by hacking into his computer using a Trojan horse. This "slow-burn" start contrasts sharply with the world's introduction to nuclear weapons technology, which claimed over 70,000 lives, most of them on the day of the explosion itself [14]. However, a limited history of past use doesn't portend less-than-existential risks in the future.

B. Resilience

A nation's second strike capacity emerges from its diplomatic and military resources.

Most obviously, even when nearly all military infrastructure has been destroyed, a state could derive help from its allies. For example, the NATO treaty [15] demands that "an armed attack against one or more of them … be considered an attack against them all." If a catastrophic cyber-attack against a NATO country is clearly attributed to an adversary, NATO members would be obliged to retaliate. In fact, the Wales Declaration [16] recognizes that "cyber defence is part of NATO's core task of collective defence."

However, some skeptics believe that it's not obvious that a state would risk bringing a war upon itself to support an ally. After all, the ally would then become equally subject to a reciprocal attack.

If diplomatic resources are inadequate, a state could still rely on its military resources. A national cyberweapons department doesn't need extensive infrastructure. In the past, deploying cyber weapons has taken teams of ten coders or less who may be distributed across the globe [17]. It may be impossible to eliminate such a small, dispersed hacker force.

An especially risk-averse state, however, could also rely on the following methods to establish credible cyber deterrence [18]:

- **Implanted software exploits:** The US has reportedly spent "hundreds of millions, maybe billions [of dollars]" on infiltrating or backdooring Iran's power grid, air defense, communications, and financial systems [19]. This is significantly different from a piece of malware loaded into a system that was already designed and functioning, such as a power grid. In contrast, implanted exploits are loaded into a system while it is being designed, unbeknownst to the designers [20]. It may seem at first that their effectiveness is limited, because deterrence requires a credible threat and, by definition, a system's designers don't know of the existence of implanted exploits. However, the existence of implanted exploits in critical systems may come to be expected as cyberweapons technology advances, such that nations feel credibly threatened.
- **Submersible data centers:** Data centers hosted on submarines can launch destructive cyber-attacks while remaining hard to detect or eliminate. The key concern of hosting a data center is managing waste heat. As much as 20 percent of the initial costs of setting up a data center is on building appropriate cooling systems [21]. Fortunately, scientists have already designed efficient cooling systems to maintain low reactor core temperatures at nuclear submarines, based on the principle of using heated coolant water to turn a propulsion turbine [22]. This cooling mechanism can be easily repurposed to dissipate waste heat from data centers. A second challenge is resisting signal jamming attacks. By using terahertz lasers that rely on novel frequency modulation techniques, submarines can design their communications systems to evade jamming attacks [23]. When they need to conduct a cyber-attack, they can simply resurface to connect to land- or satellite-based internet ports.

In summary, the diplomatic resources at a country's disposal, the ease of maintaining a small hacker force dispersed throughout a globe, and the prospect of using implanted exploits and submersible data centers makes cyber operations unusually resilient to a disarming first strike.

C. *Ease of delivery*

A cyberweapon can be usually delivered in one of two ways: using a physical carrier or via the Internet. Stuxnet, for example, had to be delivered via a physical carrier (an infected flash drive). This is because officials at the Natanz nuclear facility had taken pains to "air-gap", or isolate, their centrifuges from the Internet [24].

It is almost impossible, however, to shield critical systems such as power, sewer, healthcare, banking, and possibly air defense from the Internet. There are simply too many interactions that they must carry out with people located away from the servers hosting these systems. This leaves them vulnerable to internet-transmitted malware.

This point is not merely a theoretical one. In 2017, a cyberattack that is widely believed [25] to have been authorized by the Russian state caused the radiation monitoring system at Ukraine's Chernobyl nuclear power plant to go offline [26], and affected Ukrainian ministries, companies, and state-owned enterprises. The total damages were over $10 billion. At the time, the US Presidential Administration [27] called it the "most destructive and costly cyber-attack in history." Reference [28] notes that the attack occurred when the Ukrainian tax accounting package MeDoc's "automatic update system was [remotely] compromised and used to download and run malware rather than updates for the software."

The 2014 attack on Ukraine's national voting system [29], as well as the 2015 [30] and 2016 [31] attacks on its power grid were also caused due to internet-transmitted malware.

It is not currently known whether nuclear command-and-control chains are air-gapped. However, as the incidents described in the previous paragraph show, hackers can cause significant damage even if they don't have access to nuclear command-and-control chains, by targeting infrastructure that cannot plausibly be taken off the internet.

Due to the viability of Internet-launched attacks on critical physical systems, cyberweapons fulfill the "ease of delivery" criterion.

4. Attribution and Cyber Deterrence

In the previous section, we have seen that cyberweapons can be extremely *destructive*, *resilient* against a first strike, and *easy to deliver*, fulfilling the set of necessary criteria for conflict deterrence. In principle, then, cyberweapons could deter war.

However, their deterring ability hinges on attack attributability. If attackers believe that their actions leave visible trails, attacks could be deterred, but not if attribution is impossible. Currently, cyber-attack attribution is notoriously difficult – indeed, according to [32], "[p]erhaps the most difficult problem" in cybersecurity – due to inherent technical and legal difficulties, and the prevalence of deception.

Unlike missile strikes, cyber strikes don't leave an immediately visible trail. As [33] shows, hackers can rely on a range of techniques to make attribution difficult, including spoofing and anonymizing IP addresses [34], tampering log files, employing proxy servers or virtual private networks (VPNs), creating cover organizations, aliasing accounts, and forging credentials.

Further, hackers can route attacks across a large number of jurisdictional boundaries, sometimes necessitating transnational cooperation which can take months [35]. In the past, states have also refused to cooperate in cyber-attack investigations [36].

To add to the difficulty, hackers can execute "false flag" operations which deceive or mislead forensics experts into misattributing an attack's origin. For example, in 2018, a worm rendered vital IT infrastructure at the Winter Olympics unusable. However, this worm didn't self-destruct after the hack, as is common, leading experts to conclude that the hackers intended to be discovered. Surely enough, the malware was infused with false signatures pointing to actors who weren't involved in the operation, such as North Korea and China. This is one of the highest-profile known attempts at deceiving forensics experts [37].

However, though cyber-attack attribution is difficult, it is rarely impossible given enough time and resources. This is because even though the technical and legal challenges required in attribution are great, forensics experts frequently rely on *context*, which refers to geopolitical cues useful in tracking down the attacker. For example, experts relied heavily on context to conclude that the 2010 Stuxnet virus was jointly produced by the US and Israel [38]. The first and most obvious hint was the target state, and the targeted device; few actors would be interested in and capable of targeting Iran's nuclear centrifuges. Another clue was the scale of the attack: it chained four previously unknown security vulnerabilities, which would be collectively worth millions of dollars on the black market, a sum likely outside the budget of non-state groups at the time [20].42 In this case, knowledge of the target state, the targeted devices, and the resources poured into the attack, were all crucial to the forensics process.

Fortunately, only a few states currently have the capability to execute a catastrophic cyber-attack [40]. So, the victim could leverage contextual cues to focus its investigation on a handful of likely perpetrators.

Cyberweapons proliferation challenges the status quo. If multiple states and non-state actors acquire advanced cyberweapons capability, geopolitical deduction would become impossible, and the credible threat of retaliation would erode.

To an extent, this is already happening. For example, the 2020 data theft at the security software company Accellion was the brainchild of the hacker groups Clop Ransomware and FIN11 [41].44 They reportedly chained together four different software vulnerabilities, marking a level of sophistication and initiative never shown before by a non-state cybercriminal group. Reference [42] details how a single US hacker was able to cause a mass Internet shutdown in North Korea, an attack of a scale previously thought to be within the capability of only nation-states.

As another indicator of the "democratization" of cyber offense capabilities, half of the over 200 major state-executed cyber-attacks since 2009 involved malware tools that could be easily purchased on the dark net by private actors. Only about 20% of the attacks involved weapons of some sophistication [43].The gap between state cyberwar wings which receive billions in funding, and ragtag cybercrime groups, is rapidly closing.

As [44] notes, it may not matter much whether firms are able to attribute attacks. Regardless of the perpetrator, firms should focus on strengthening cyber defense and resilience. States, on the other hand, should treat the ability to reliably attribute attacks as a public good, since it maintains international security. Otherwise, the default state of the world would be constant, unattributable cyberwar.

Cyberweapons can help deter state-led aggression – but not if nation-states' ability to attribute catastrophic cyber-attacks erodes.

5. Policy Recommendations

As the previous section showed, cyber deterrence faces grave threats. How should states respond?

If the discussion throughout the paper is correct, then a state doesn't need great cyber "shields" to deter catastrophic cyber-attacks. It just needs sharp cyber "swords" (and the ability to attribute attacks).

As an analogy, no nuclear power currently has a missile defense system capable of defending against a full-fledged nuclear first strike. However, they are reasonably certain that they will not be at the receiving end of a nuclear strike. This is because nuclear deterrence works: a first strike spells mutually assured destruction.

Currently states and charitable foundations concerned about international security over-invest in cyber defense, and underemphasize cyber attribution. There are two ways to strengthen attribution: directly via cyber forensics, and indirectly via reducing cyberweapons proliferation.

D. Cyber forensics

The US Nuclear Forensics and Attribution Act [45] aims to "develop nuclear forensics capabilities to permit attribution of the source of nuclear material" through research fellowships and the standardization of protocols for exchanging data with international bodies. It would be useful to support the field of cyber forensics with similar legislative action worldwide.

However, the key constraint in timely cyber forensics is not a dearth of technical competence, but the lack of an international framework to attribute cross-jurisdictional attacks [46]. It would be useful to establish transnational agreements for sharing data relevant to cyber forensics. There should also be clearly defined consequences for non-cooperation. States would have an incentive to join such an agreement, as they would get access to data important for attributing and thus deterring cyber-attacks on their own infrastructure.

It must be noted that countries and foundations that invest in cyber forensics research should take care not to accidentally advance cyber offensive capabilities by proliferating cyberweapons that have a dual offensive-defensive function (such as war dialers, port and vulnerability scanners, password crackers, sniffers, and network administration and monitoring tools) [47]. Additionally, they must ensure that advanced attribution capability is not misused by authoritarian regimes to crack down on dissidents.

E. Cyberweapons nonproliferation

As we noted earlier, state cyber hacking groups remain the best-funded, most advanced users of cyberweapons on the planet. Hence, the likeliest vector of cyberweapons proliferation is theft of these tools by groups such as the Shadow Brokers, who stole weaponized exploits from the NSA which were used to cause over $8 billion in damages globally [48]. To counter this threat, national intelligence communities urgently need to invest in the research and adoption of information assurance and security best practices.

Further, states need to curb the black market for cyber weapons. To do so, they may leverage existing domestic safety acts and international export controls on software vulnerabilities such as the 1996 Wassenaar Arrangement, but it is also important to bolster the prosecutorial framework to deter vendors of dangerous exploits [49].

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] Straub, J. (2019, August 16). A cyberattack could wreak destruction comparable to a nuclear weapon. The

Conversation. https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173

[3] Goldrick, J., Clarke, P., Barrett, T., & Davis, M. (2020). Why submarines? In P. Jennings & M. Hellyer (Eds.), Submarines: Your questions answered(pp. 4–19). Australian Strategic Policy Institute. http://www.jstor.org/stable/resrep26897.5

[4] Watson, D. E. (2017). Rethinking the US Nuclear Triad. Strategic Studies Quarterly, 11(4), 134–150. http://www.jstor.org/stable/26271637

[5] Department of Defense Law of War Manual (pp. 1015–1016). (2016). Government Printing Office. https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190 (Original work published 2015)

[6] Dunleavy, B. P. (2022, June 1). Pacemakers, insulin pumps can be hacked, experts say. UPI. https://www.upi.com/Health_News/2022/06/01/medical-devices-pacemakers-cybersecurity/7041653656330/

[7] Knake, R. K. (2017). A Cyberattack on the U.S. Power Grid. Council on Foreign Relations. https://www.cfr.org/report/cyberattack-us-power-grid

[8] Gisel, L., & Olejnik, L. (2018). The potential human cost of cyber operations. In ICRC.org. International Committee of the Red Cross (ICRC). https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf

[9] Kumakura, T. (2008, April 27). North Koreans may have died in Israel attack on Syria, NHK says. Bloomberg. https://web.archive.org/web/20121103011551/http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aErPTWRFZpJI&refer=japan

[10] Fulghum, D. A., & Wall, R. (2007, November 26). Israel shows electronic prowess. Aviation Week. https://aviationweek.com/israel-shows-electronic-prowess

[11] Hemmer, P. T. (2013). Deterrence and cyber-weapons (p. 28) [Master's Thesis]. https://calhoun.nps.edu/bitstream/handle/10945/32836/13Mar_Hemmer_Patrick.pdf?sequence=1&isAllowed=y

[12] Stoutland, P. O., & Pitts-Kiefer, S. (2018). Nuclear weapons in the new cyber age. Nuclear Threat Initiative. https://www.nti.org/wp-content/uploads/2018/09/Cyber_report_finalsmall_Zg5TarX.pdf

[13] Futter, A. (2018). Hacking the Bomb. Georgetown University Press.

[14] Carr, J. (2013). The misunderstood acronym: Why cyber weapons aren't WMD (p. 35). Bulletin of the Atomic Scientists, 69(5), 32–37. https://doi.org/10.1177/0096340213501373

[15] Wellerstein, A. (2020, August 4). Counting the dead at Hiroshima and Nagasaki. Bulletin of the Atomic Scientists. https://thebulletin.org/2020/08/counting-the-dead-at-hiroshima-and-nagasaki/

[16] The North Atlantic Treaty. (1949). https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[17] Wales Summit Declaration. (2014). https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[18] Kushner, D. (2013, February 26). The Real Story of Stuxnet. IEEE Spectrum; IEEE Spectrum. https://spectrum.ieee.org/the-real-story-of-stuxnet

[19] Pattara, Peter R. (2021). Cyber Mutually Assured Destruction & Counterproliferation for the 21st Century: "How I stopped worrying and learned to love the software exploit.". Liberty University Journal of Statesmanship & Public Policy: Vol. 1: Iss. 2, Article 6. https://digitalcommons.liberty.edu/jspp/vol1/iss2/6

[20] Szoldra, P. (2016). The US could have destroyed Iran's entire infrastructure without dropping a single bomb. Business Insider. https://www.businessinsider.com/nitro-zeus-iran-infrastructure-2016-7

[21] Gibney, A. (Director). (2016). Zero Days. Magnolia Pictures.

[22] Zhang, M. (2022, May 30). How much does it cost to build a data center? Dgtl Infra. https://dgtlinfra.com/how-much-does-it-cost-to-build-a-data-center

[23] Nuclear submarines and aircraft carriers. (2018, November 30). United States Environmental Protection Agency. https://www.epa.gov/radtown/nuclear-submarines-and-aircraft-carriers

[24] Dunn, A., Poyser, C., Dean, P., Demić, A., Valavanis, A., Indjin, D., Salih, M., Kundu, I., Li, L., Akimov, A., Davies, A. G., Linfield, E., Cunningham, J., & Kent, A. (2020). High-speed modulation of a terahertz quantum cascade laser by coherent acoustic phonon pulses. Nature Communications, 11(1). https://doi.org/10.1038/s41467-020-14662-w

[25] Kushner, D. (2013, February 26). The Real Story of Stuxnet. IEEE Spectrum; IEEE Spectrum. https://spectrum.ieee.org/the-real-story-of-stuxnet

[26] Greenberg, A. (2018, August 21). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[27] Griffin, A. (2017, June 27). "Petya" cyber-attack: Chernobyl's radiation monitoring system hit by worldwide hack. The Independent. https://www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html

[28] Statement from the Press Secretary – The White House. (2018). Archives.gov; The White House. https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/

[29] Wakefield, J. (2017, June 28). Tax software blamed for cyber-attack spread. BBC News; BBC News. https://www.bbc.com/news/technology-40428967

[30] Pavel Polityuk. (2019, January 25). Exclusive: Ukraine says it sees surge in cyber-attacks targeting election. U.S. https://www.reuters.com/article/us-ukraine-cyber-exclusive-idUSKCN1PJ1KX

[31] BBC. Hackers caused power cut in western Ukraine. (2016, January 12). BBC News. https://www.bbc.com/news/technology-35297464

[32] Greenberg, A. (2019, September 12). New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. WIRED; WIRED. https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

[33] Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: what everyone needs to know (p. 73). Oxford University Press.

[34] Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

[35] Vlajic, N., Chowdhury, M., & Litoiu, M. (2019). IP Spoofing In and Out of the Public Cloud: From Policy to Practice. Computers, 8(4), 81. https://doi.org/10.3390/computers8040081

[36] Clapper, J. R. (2015). Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee (p. 2). https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

[37] Graham, B. (2005, August 25). Hackers attack via Chinese web sites. The Washington Post. https://www.washingtonpost.com/archive/politics/2005/08/25/hackers-attack-via-chinese-web-sites/03559eb7-4e56-40bf-b406-8198bd1e1131/

[38] Greenberg, A. (2019, October 17). The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History. WIRED; WIRED. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/

[39] Nakashima, E., & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

[40] Morgan, C. (2021, June 1). Cyber-attacks: the challenge of attribution and response. Digital Shadows. https://www.digitalshadows.com/blog-and-research/cyber-attacks-the-challenge-of-attribution-and-response/

[41] Seals, T. (2021, February 22). Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11. Threatpost. https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/

[42] Greenberg, A. (2022, February 2). North Korea hacked him. So he took down its Internet. WIRED. https://www.wired.com/story/north-korea-hacker-internet-outage/

[43] McGuire, M. (2021). Nation States, Cyberconflict and the Web of Profit. In HP Threat Research. https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf

[44] Fier, J. (2021, October 18). In cyberwar, attribution can be impossible — and that's OK. Dark Reading. https://www.darkreading.com/analytics/in-cyberwar-attribution-can-be-impossible---and-that-s-okay

[45] Nuclear Forensics and Attribution Act, (2010). https://www.govinfo.gov/app/details/PLAW-111publ140/summary

[46] Clark, D. D., & Landau, S. (2010). Untangling Attribution. In Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (pp. 25–40). The National Academies Press. https://nap.nationalacademies.org/read/12997/chapter/4

[47] Denning, D. (2000). Reflections on Cyberweapons Controls. Computer Security Journal, 16(4), 45–53. https://faculty.nps.edu/dedennin/publications/Reflections_on_Cyberweapons_Controls.pdf

[48] Cimpanu, C. (2018, May 11). One Year After WannaCry, EternalBlue Exploit Is Bigger Than Ever. BleepingComputer. https://www.bleepingcomputer.com/news/security/one-year-after-wannacry-eternalblue-exploit-is-bigger-than-ever/

[49] Stockton, P. N., & Golabek-Goldman, M. (2013). Curbing the Market for Cyber Weapons. Yale Law & Policy Review, 32(1), 239–266. http://www.jstor.org/stable/23736234