CYBER WARFARE & TERRORISM

Jean-Jacques Halans

CSU March 16 2022

Introduction

While researching this essay, the TV is on in the background and we are into the third day of the Russian invasion in Ukraine. As reported early in the year (*Cyber attack hits Ukraine as United States intelligence warns Russia preparing to invade*, 2022), Ukraine had already been under an increased, sustained cyber-attack (*Australia joins US and UK, blaming Russia for cyber attacks against Ukraine*, 2022), in a ‘hybrid’ war (*Ukraine claims Russia behind cyber attack in 'hybrid war'*, 2022) in the lead up to Russia’s invasion, as Australia promised Ukraine cyber support and cyber training (Dziedzic, 2022).

As the word “cyber” is thrown around by the public broadcaster, it conjures up images of hackers and code scrolling across a computer screen, reminiscent of The Matrix. “Cyber”, unlike cipher (or cypher), is hardly a technical term, originating in art and popular culture (Vocabularist, 2016), so what are we to understand as “Cyber Warfare and Terrorism”?

Cyber Warfare and Terrorism

The word "cyberspace" was introduced to a wide audience through the science fiction short story "Burning Chrome" by popular author William Gibson in 1982 (Popova, 2014). As Gibson reminisces in the 2013 NYPL interview

> "*I wanted that sense of other realm, a sense of agency within my daily life, looking for bits and pieces of reality that could be cobbled into the arena I needed.*" (Gibson, 2013, 0:38-0:53),

a realm different to the physical space, our inner space or Outer Space. "Cyberspace" was earlier used by the Danish "Atelier Cyberspace" artists Susanne Ussing and Carsten Hoff (Andersen, 2019) in their 1969 dry transfers and photolithography work, as "*studies in cybernetics and open systems, that change behaviour in response to what they are influenced by.*" (Ussing and Hoff, 1969).

These artists' description of their work could easily form the basis of a definition of warfare and terrorism in cyberspace:

> our globally interconnected information and communication technology platform as ***open system*** that ***changes behaviour*** unexpectedly and with dire consequences, ***in response*** *to* a cyber-attack, a nefarious ***outside influence*** by a threat actor.

An early definition of "cyberwar" revolves around war about "knowledge", "*about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries*" (Arquilla & Ronfeldt, 1997, p42 - p44), with an end goal of destroying, if not at least disrupting the adversaries' communications systems and information flow.

From a US legal perspective, one definition of "cyber warfare" is the act of warfighting in the cyber domain, covered by US Code Title 10, under the command of a US military officer as part of or in support of a military operation in some other domain (be it land, air, sea or space) (Oakley, 2019, Ch. 3). But as Oakley adds, even though the US acknowledges its role in Title 10 activity, like launching Tomahawk missiles, often it doesn't admit any cyber involvement in those operations.

Take for example Stuxnet in 2010, probably one of the most successful targeted cyber-attacks to date, specifically developed to cripple Iran's uranium enrichment facilities ("Stuxnet," 2020), though in the end only temporary, and without casualties. It was generally attributed to be a joint US/Israeli operation, but no country has claimed the cyber-attack (Chen, 2010). Stuxnet was a formidable offensive cyber weapon, that highlights the capability of cyber-attacks to affect critical infrastructure, yet with limited and temporary impact only.

When Merck Pharmaceuticals fell victim to the NotPetya ransomware attack in 2017, it asked its insurance company to pay out the property insurance policy it had, which the insurer denied because of the "cyber war" clause in the policy. Two years later, a judge sided with Merck as there was not an actual formal war between nations, in this case between Russia, to whom NotPetya was attributed to, and the US, hence there can’t be a cyber war (Ikeda, 2022).

Maybe a “cyber terrorism” insurance clause would have made more sense, defined by Denning as “*unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives… [and] should result in violence against persons or property, or at least cause enough harm to generate fear*” (Denning, 2000). Years later we also tend to include the online recruitment, radicalization, planning and financing of terrorist groups in this definition (*The UK Cyber Security Strategy*, 2011). At this point there’s a fine line between cyber terrorism and cyber-crime.

When indiscriminate ransomware hits 300.000 targets across 150 countries demanding $300 to release your data, this would deliver a decent financial windfall to any online organised crime syndicate. But when WannaCry ransomware hits the UK’s NHS, a critical health service, locking NHS staff out of patient records and medical equipment (Schmitt and Fahey, 2017), this could become potentially life-threatening. Especially when combined with a terrorist bomb attack. But that wasn’t the case, and again WannaCry turned out be an expensive and disruptive act of sabotage, attributed as being “sponsored by” North Korea.

Cyber-attacks are dependent on software (and hardware) vulnerabilities or misconfiguration, and often use a combination of flaws. You only need to keep track of the Common Vulnerabilities and Exposures database, currently at 171667 entries at the time of writing (CVE, 2022), to realize there will never be an opportunity left unused to exploit these software flaws, either by state actors, hacktivists, cyber criminals or terrorists.

It gets complicated though when a state actor like the US’ NSA sits on an undisclosed 0day Windows vulnerability called EternalBlue (later, once disclosed, registered as CVE-2017-0144), which it allegedly used for 5 years against US adversaries for intelligence gathering (Schulze and Reinhold, 2018), but then “lost” this to a hacker collective called "Shadow Brokers" which then resulted in the creation of first the WannaCry malware, and eventually also NotPetya (Fruhlinger, 2017).

Conclusion

So far there hasn’t been a documented high-tech Pearl Harbour or Hiroshima, and it may never happen (Rid, 2012). WannaCry and NotPetya could have been avoided if people kept their Windows systems up to date with the latest security patches. Stuxnet would have been useless if the malware wasn’t plugged into an Iranian network connected device. As technology evolves, so will cyber-attacks and, by definition, cyber warfare and terrorism. But the effective cyber-attack, worthy of a cyber warfare or terrorism designation, remains elusive. Maybe the true cyberwar happens when state actors, like NSA, hacktivists and other cyber warriors engage each other in cyberspace to extract “knowledge” (like the EternalBlue flaw) to then develop cyber-attack tools?

References

Andersen, T. R. (2019). Cyberspace Revisited: A Radial Reading of William Gibson's "Burning Chrome". *Journal of American culture*, *Vol.42 (2)*(2019-06). https://doi.org/10.1111/jacc.13019

Arquilla, J., & Ronfeldt, D. (1997). CYBERWAR IS COMING. In (1 ed., pp. 23). RAND Corporation. https://doi.org/10.7249/mr880osd-rc.7

Australia joins US and UK, blaming Russia for cyber attacks against Ukraine. (2022). ABC. https://www.abc.net.au/news/2022-02-21/australia-joins-us-and-uk-to-blame-russia-for/13763218

Chen, T. M. (2010). Stuxnet, the real start of cyber warfare? *IEEE network*, *24*(6), 2-3. https://doi.org/10.1109/MNET.2010.5634434

CVE. (2022). *CVE*. https://www.cve.org/

Cyber attack hits Ukraine as United States intelligence warns Russia preparing to invade. (2022). Reuters, AP. https://www.abc.net.au/news/2022-01-15/us-intelligence-warns-russia-laying-groundwork-to-invade-ukraine/100758744

Denning, D. E. (2000). Cyberterrorism: The Logic Bomb versus the Truck Bomb. *Global dialogue (Nicosia, Cyprus)*, *2*(4), 29.

Dziedzic, S. (2022). *Australia promises cyber support to Ukraine as Russian forces array along its borders*. ABC. https://www.abc.net.au/news/2022-02-21/ukraine-australia-cyberattack-russia-war-cybersecurity/100846870

Fruhlinger, J. (2017). The 5 biggest ransomware attacks of the last 5 years: From CryptoLocker to WannaCry and NotPetya, these attacks illustrate the growth of ransomware. *CSO (Online)*.

Gibson, W. (2013, July 17). *The Origin of "Cyberspace"* [Video]. YouTube. https://www.youtube.com/watch?v=ae3z7Oe3XF4

Ikeda, S. (2022). *"Cyber War" Exception Struck Down in Merck's Battle With Insurance Company Over NotPetya Attack*. CPO Magazine. https://www.cpomagazine.com/cyber-security/cyber-war-exception-struck-down-in-mercks-battle-with-insurance-company-over-notpetya-attack/

Oakley, J. G. (2019). *Waging Cyber War Technical Challenges and Operational Constraints* (1st 2019. ed.). Apress. https://doi.org/10.1007/978-1-4842-4950-5

Popova, M. (2014). *How William Gibson Coined "Cyberspace".* The Marginalian. https://www.themarginalian.org/2014/08/26/how-william-gibson-coined-cyberspace/

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5-32. https://doi.org/10.1080/01402390.2011.608939

Schmitt, M., & Fahey, S. (2017). *WannaCry and the International Law of Cyberspace*. JustSecurity.org. https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/

Schulze, M., & Reinhold, T. (2018). Wannacry About the Tragedy of the Commons? Game-Theory and the Failure of Global Vulnerability Disclosure. European Conference on Cyber Warfare and Security, Reading.

Stuxnet. In. (2020). *Britannica Academic*. https://academic-eb-com.ezproxy.csu.edu.au/levels/collegiate/article/Stuxnet/544278

The UK Cyber Security Strategy. (2011). gov.uk. https://www.gov.uk/government/publications/cyber-security-strategy

Ukraine claims Russia behind cyber attack in 'hybrid war'. (2022). AP. https://www.abc.net.au/news/2022-01-17/ukraine-claims-russia-behind-cyber-attack-in-hybrid-war/100760370

Ussing, S., & Hoff, C. (1969). *Cyberspace*. https://primer.dk/onsite/Projects/Life-Without/Susanne-Ussing-Cyberspace-1969

Vocabularist. (2016). *How we use the word cyber.* BBC. https://www.bbc.com/news/magazine-35765276.amp