SS334 Discussion Forum 1

Jonathan Lam

2022/03/27

Technology and the internet has opened the door for a lot of nontraditional goods to study. For example, Bitcoin and other cryptocurrencies may be considered nonexcludable and rival (rival because of the finite size of the Bitcoin pool), privately-owned websites may be considered excludable and nonrival, and access to the Internet itself (which is ultimately tied to public infrastructure, and where bandwidth is almost inconsequential) is nonrival and non-excludable (a public good). Along the same lines, information is a public good, and the Internet is arguably its largest disseminator.

It's unsurprising that as the dependence on the Internet grows, the value of networked systems and the data stored on such systems has increased exponentially, and with it the frequency and cost of cyberattacks.

If we briefly consider the U.S.A., there are a wealth of statistics about cybersecurity attacks. For example, IBM and the Potemon Institute estimate that the average cost of a data breach in the U.S.A. in 2021 was $4.24million, at6$ trillion annually [1]. This are losses greater than the 3rd largest GDP in the world (Japan, at \$5.06 trillion) [2].

Turning our focus to the Russia-Ukraine conflict, it's clear that proper utilization of the Internet, or the advantages gained by defenes and attacks through the digital medium of networked computers, have very real effects on the outcome of war and on the economy.

For example, take the following cases, reported by law firm Baker Hostetler, which specializes in data issues [3]:

- In 2015, Russian hackers hacked the Ukranian power grid, causing major outages.

- In 2017, the NotPeya Russian malware aimed at Ukraine's networks caused billions of dollars of damages globally.

- As retaliation against U.S. sanctions, some Russian-based ransomware groups such as Conti have recently posted their victims's data online, even after the victims have paid the ransom.

- The Ukranian government has asked for volunteer hackers, who have successfully launched some attacks against major Russian websites and against the train systems of Russia's ally Belarus.

- There was a major leak of internal infrastructure and data of a major Russian ransomware group called Conti by pro-Ukraine members, severely jeopardizing the group's activities.

Another example of hacking, this one by the hacking group Anonymous, has become widely known. A report by security company Security Discovery posted a report of their attempt to fact-check the claims by Anonymous, and they verified 92 compromised Russian databases of governmental websites, multiple hacked Russian state TV stations, and denial-of-service attacks against major Russian state websites such as RT [4].

Other communications-related failures that have a direct impact on military compaigns includes carelessness due to the use of personal phones or unencrypted radios, which have reputedly caused multiple Russian officials to be killed [5].

These examples probably only represent a tiny fraction of the true extent of the cyberattacks related to this war, many of which will only be declassified or discovered at a much later time. Cybersecurity mistakes or attacks have probably caused billions of dollars in both military blunders and in company losses in Russia, Ukraine, and in other nations due to retaliatory measures – and this is on top of traditional war-time costs.

One of the factors that makes information and the Internet particularly interesting are that they are public goods, that any state cannot afford to lose access to. The benefit of cutting a nation's Internet completely off from the rest of the world is that you would get some protection from cybersecurity attacks, but this is far outweighed by the cost of inconveniences for ordinary citizens and by losing free access to highly valuable information. Of course, this doesn't stop nations from attempting to control media, as is famous with China's "Great Firewall"[6], and presumably is similar to what Russia may be attempting now with its state media. As we mentioned in class, privatization is one way to solve issues when there are uncooperative agents with an excludable good. And the Internet is not just full of uncooperative agents; it's full of malicious ones, especially at times of war.

The best policy recommendation that I could give is to increase investment in cybersecurity resources and education. The first would be a short-term benefit, and the latter a long-term benefit, both for wartime and peacetime. There are numerous issues with cybersecurity today: while some are fundamentally related to protocols or systems not designed to be secure (e.g., unencrypted email) and are thus "unfixable" without designing new protocols, many cybersecurity issues exist out of human error or even social engineering, which we can train people to protect against.

Bibliography

[1]: Tunggal, Abi Tyas. “What Is the Cost of a Data Breach in 2021?” Upguard, Upguard, Inc., 23 Feb. 2022, https://www.upguard.com/blog/cost-of-data-breach.

[2]: Silver, Caleb. “The Top 25 Economies in the World.” Investopedia, Investopedia, 4 Feb. 2022, https://www.investopedia.com/insights/worlds-top-economies/.

[3]: Koller, M. Scott. “Impact of the Ukraine/Russia Conflict on Cybersecurity in the United States.” Baker Data Counsel, Baker and Hostetler LLP., 16 Mar. 2022, https://www.bakerdatacounsel.com/data-security/impact-of-the-ukraine-russia-conflict-on-cybersecurity-in-the-united-states/.

[4]: Pitrelli, Monica Buchanan. “Anonymous Declared a ’Cyber War’ against Russia. Here Are the Results.” CNBC, CNBC, 16 Mar. 2022, https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html.

[5]: Booth, William, et al. “Russian Generals Are Getting Killed at an Extraordinary Rate.” The Washington Post, WP Company, 27 Mar. 2022, https://www.washingtonpost.com/world/2022/03/26/ukraine-russan-generals-dead/.

[6]: Chan, Conrad, et al. “China’s Great Firewall.” Free speech vs. Maintaining Social Cohesion. Stanford, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.