Cyber Security

Gawdat Bahgat

Outline

- Introduction
- Terminology
- Cybercrime/ransomware
- Cyber deterrence
- Digital cold war
- Undersea fiber-optic cables
- China
- US
- Conclusion: the way forward

Introduction-1

- The digitization of society has created tremendous progress & empowerment, but it also has a dark side – cyber crime & cyber warfare
- Cyber operations are ideal given their opacity, lack of clear norms & inadequate defenses.
- The asymmetric nature of cyber capabilities means smaller countries can punch above their weight
- Cyber power is considered as a domain in its own right, not as complementary to other forms of power. Cyberspace is already the 5th domain after space, sea, land & air.

Introduction-2

- Cyber realm is “offense-dominant”: Hacking into networks is easier, faster & cheaper than protecting or patching them. Most networks are meant to enable information sharing, making it difficult & potentially self-defeating to prevent access.
- Annual global cybersecurity investment has doubled from $80 billion to $160 billion since 2016. These investments are yielding ever-diminishing returns.
- The cost of network attacks is doubling every few years & could reach $6 trillion in 2021

Terminology-1

- Critical infrastructure: are systems & assets, physical & virtual, so vital that their incapacity or destruction would have a debilitating impact on national defense, economic prosperity, public health & safety.
- Hacking: gaining an unauthorized access to a computer system or network.
- Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files & the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. They often target & threaten to sell or leak data or authentication information if the ransom is not paid.

Terminology-2

- Cyber espionage is a cyber operation to obtain unauthorized access to sensitive information through covert means.
- Cyber operation is organized activities in cyberspace to gather, prepare, disseminate, restrict or process information to achieve a goal
- Cyberwar refers to an act of aggression, committed through a digital network, meant to cause damage in the real world, either to civilian or military targets, in order to force a sovereign state to act or refrain from acting.

Terminology-3

- Internet governance refers to the development & application by governments, the private sector & civil society of shared principles, norms, rules, decision-making procedures & programs that shape the evolution & use of the internet.
- Cyber policy is any measure by public or private entities regarding human or non-human activity aimed at achieving intended effects in and through cyber space

Cyber Crime – Ransomware-1

- Cyber crime is typically seen as a profit-driven, non-violent white-collar crime.
- Ransomware is not just financial extortion, it is a crime that transcends business, government, academic & geographic boundaries
- Most ransomware criminals are based in countries that are unwilling or unable to prosecute them
- In 2020 nearly 2,400 US-based governments, healthcare facilities & schools were victims of ransomware – a steady increase in the number of attacks and damaging economic impact

Cyber Crime – Ransomware2

- Cyber insurance industry sells policies to firms to cover losses in the event of a ransomware attack including business interruption losses, data restoration costs, incident response costs & ransom payment.
- The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin & other cryptocurrencies.
- Carrying out a ransomware attack does not require technical sophistication. “Ransomware as a service” (RaaS) is a business model that provides capabilities to would-be criminals who do not have the skills or resources to develop their own malware.
- Victims may worry about reputational harm.

Cyber Crime – Ransomware3

- Ransomware has moved from an economic nuisance to a national security & public health & safety threat.
- As such it requires stepped-up efforts by both government & private sector
- It is a widely accepted international norm that cyberattacks by states on critical national infrastructure are off-limits.
- The attack on Colonial Pipeline shows that disrupting critical national infrastructure is not an option only available to states & that it is time to re-assess the intersections between cybersecurity & cybercrime.

Cyber crime – Ransomware4

- In US, much of critical infrastructure is owned & operated by the private sector
- President Biden signed executive order https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

Cyber deterrence-1

- Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit.
- The primary goal for nuclear deterrence is zero use not the case in cyber domain
- Arguing that deterrence does not work at all in cyberspace ignores what already does not happen (i.e. attacks on critical infrastructure)
- The problem is not whether it works, rather it is whether to expand it to work against a broad set of cyber activities

Cyber deterrence-2

- Anonymity in cyberspace makes it more difficult for states to assess an adversary’s capabilities, making deterrence difficult
- Cyberspace is not borderless, it is not entirely divorced from physical world.
- Cyber deterrence does not seek zero use rather it aims for risk management, not to eliminate but to reduce cyberattacks.

Digital cold war-1

- States are trying to shape, influence & control the future design & governance of the internet
- Russia, China & some other states: Great state control model
- West: multi-stakeholder model (governments, private sector & individuals)
- Competition for control over the technologies that physically underpin the future of cyberspace (microchips, computer assembly 5G, cloud architectures, cables & routers
- International law applies to cyber, but it is primarily a legal order for states

Digital cold war-2

- The future cyber resilience of every state depends on the physical infrastructure underpinning the global internet, how it is built & by whom
- US argues that the integration of Chinese technology in national digital ecosystems will have significant consequences for defense cooperation with US
- US & allied countries still dominate global markets with 42 of the top 50 telecoms & tech companies compared with China’s 8
- China aims to become a technological superpower

Digital cold war-3

- This includes AI, super-apps, 5G, smart cities, surveillance technology & shape the global rules of tech governance
- China is exporting its vision of internet governance (cyber sovereignty)
- State cooperation model vs. multi-stakeholder model
- China’s model promotes economic benefits of internet while neutering the risk of protesting online
- China provides more financing for ICT in Africa than all multilateral agencies & Western countries do across the continent

Digital cold war-4

- China is the world’s major supplier of rare earths minerals
- China is the world’s largest semiconductor market, but 80% of the chips are either imported or produced by foreign companies in China. The industry is dominated by US, Japan & the Netherlands
- The Clean Network (clean carrier, apps, store, cloud, cable, path) 2020
- Russia: “sovereign RuNet” 2019, an alternative to global internet
- EU: EU Cybersecurity Strategy, Dec 2020. European Union Agency for Network & Information Security (ENISA) & European Cybersecurity Organization (ECSO)

Digital Cold War-5

- UN created 2 organizations to propose norms and rules to govern cyberspace – the 193-member Open-Ended Working Group (OEWG) & the 25-member Group of Governmental Experts (GGC). So far no agreement has been reached.

Undersea fiber-optic cables-1

- The infrastructure that makes the internet work is a focus of geopolitical competition
- 95% of intercontinental global data transmissions rely on undersea cables.
- They are often constructed by multinational consortiums with no single legal framework to govern their use
- There must be cooperation among like-minded countries in leading & managing their construction
- Currently US & China are the main players & rivals

Undersea fiber-optic cables-2

- Beijing considers digital infrastructure to be no longer just a question of business, but a critical part of Chinese foreign policy
- Currently all undersea cables transiting between Europe & Asia pass through Egypt

China-1

- Internet was introduced into China in late 1980s/early 1990s
- China’s digital economy was valued at $6 trillion in 2020, accounting for 38.6% of the GDP
- The Great Firewall: the combination of laws, censorship & digital surveillance that forms the basis of Beijing’s control over the internet in China
- Digital Silk Road (DSR): Digital infrastructure is rapidly replacing China’s former focus on traditional overseas infrastructure projects. DSR-related projects have been carried out/planned in 137 countries

China-2

- Chinese leaders warn domestic audiences of the dangers that stem from reliance on foreign technology
- “Without cyber security, there will be no national security.”
- “Those who set the standards, dominate the world.”
- President Xi introduced the concept of a “cyber great power” in 2014

US-1

- Cyber Deterrence Initiative (CDI) 2018: The US will work closely with allies in responding to attacks including through intelligence-sharing.
- Joint Cyber Defense Collaborative (JCDC) 2021 will bring together public & private sector entities to unify deliberate & crisis action planning while coordinating the integrated execution of these plans.
- Cybersecurity & Infrastructure Security Agency (CISA) 2018
- US digital economy is the biggest in the world, 60% of GDP
- Clean Network Initiative (include carriers, applications, app stores, cloud, paths & undersea cables)

US-2

- US has designated information security as a government-wide high-risk area since 1997
- Each year, the federal government spends more than $100 billion on IT & cyber-related investments
- National Security Agency (NSA) 1952 is the only US government organization with the vast capabilities to conduct both cyber defense & cyber offense at home & abroad
- Cybersecurity & Infrastructure Security Agency (CISA), 2018, Dept of Homeland Security

US-3

- Internet has evolved from a project sponsored by DoD in the 1960s, ARPANET, consisted of a network of supercomputers that allowed for information sharing among a number of universities & research institutes located across the US
- 2010 Cyber Command was established as a sub-unified command subordinate to Strategic Command
- DoS: 2011 Office for the Coordinator for Cyber Issues was established
- Intelligence: For the first time in history cyber security threats were ranked at the top of threats to national security

US-4

- Cyber Command was elevated to a Unified Combatant Command 2018
- 2018: National Cyber Strategy of the United States & Department of Defense Cyber Strategy
- 2020: DoS, the Office was elevated to the Bureau of Cyberspace Security & Emerging Technologies (CSET)

Conclusion – Way forward-1

- Cybersecurity requires an educated & skilled workforce, complemented by effective public-private relationships, whole-government & whole-society approach (government, private sector, academia), civilian-military partnership & cyber hygiene
- Consensus on global norms & rules to govern cyber domain is needed
- A new digital architecture is taking form. It will shape communications & resource flows, security & prosperity, global norms & information. It will inform the international balance of power & the ways in which power can be deployed within that balance

Conclusion – Way forward-2

- Covid-19 has made tighter state control of online freedom of expression more attractive to many governments

Documents & Sources-1

- National Cyber Strategy of the United States of America https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- Department of Defense Cyber Strategy https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
- Cyber Diplomacy Act of 2019 https://www.congress.gov/bill/116th-congress/house-bill/739
- FBI Cyber Strategy https://www.ic3.gov/Media/PDF/Y2020/PSA201008.pdf

Documents & Sources-2

- National Security Agency https://www.nsa.gov
- Cybersecurity & Infrastructure Security Agency https://www.cisa.gov
- Clean Network https://2017-2021.state.gov/the-clean-network//index.html