LCDR Patrick Ryan, USN (Retired)

President, Tennessee World Affairs Council

https://www.TNWAC.org

Email: PatRyan@TNWAC.org

Cell: 931-261-2353

Presentation Available: http://www.slideshare.net/TNWAC
Cyber Stuff – Definition of Terms

- Cyberwar - The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

- ‘cyberwar is asymmetric, which means it benefits lesser military powers as much as military goliaths’

- Conventional usage – more broad, umbrella term for a variety of activities

- Measures and Countermeasures
Geo Politics and Pivots

• Andres Article – “Cyber Conflict and Geopolitics”
• Mahan – the “Periphery,” maritime dominance
• Mackinder – the “Hearthland,” continental lines of communications
• Rise and fall of great powers
• Cyber as a paradigm shift or a tool of power competition?
U.S. Cyber

• 1988 – The “Morris” worm debuts
• 1990s – Growing recognition of Cyber threats
• 2013 – Executive Order – Improving Critical Infrastructure Cybersecurity
• 2014 -- Cyber National Mission Force created at NSA / Cyber Command – “to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.”
• 2018 – Cybersecurity and Infrastructure Security Act
Great Power Competition - Russia

• Russian Federation
  • Economy – Declining; GDP of Italy
  • Military – Modernizing, Strategic Nuclear Peer
  • Political – Uncertain
  • Intentions – “Near Abroad”; Disrupt West
Great Power Competition - China

- People’s Republic of China
- Economy – Soaring
- Military – Rising, Prospective Peer Competitor
- Political – Solidification of Communist Party Rule
- Intentions – Global Superpower Challenger
Case Study: Estonia

- Disabled web sites of government ministries, political parties, newspapers, banks and companies.
- First case of state vs state cyberwar.
- NATO dispatched cyber experts, but NATO doctrine did not define cyber attacks as military action, so no invocation of Article V.
- Resulted in creation of the “data embassy” – data stored abroad.
Case Study: Russia
Election / Social “Meddling”

- Long history of US-Russian / Russian-US influence operations
- 2016 Election Cycle
  - Oct 2016 – Intel Community – charged Russia
  - Jan 2017 – Intel Community – aimed to assist Trump
  - July 2017 – US indicts 12 GRU officers
- Russian Aims
  - Harm Clinton Campaign
  - Aid Trump Campaign
  - Increase political discord
- Response – Special Counsel, Congress, POTUS
  - Ambivalence
- Impact on 2018, 2020 ???

GRU – Main Intelligence Directorate of the Russian General (Military) Staff
Case Study: China/Office of Personnel Management

- Chinese hackers attacked OPM in 2014-15
  - Compromised 21.5 million government employees, applicants
  - 30-years of information including SSNs, fingerprint data, banking info, assignments, training history and other personal data
  - Sensitive data on officials, military, diplomats, and others = compromise
- FBI arrested Shanghai based “GoldSun” in 2017 for developing the malware used against OPM and private firms
Case Study: China / Huawei

- Chinese Govt relationship with Huawei – subsidies / ties
- International attraction of Huawei gear = $$$
- International attraction of Huawei gear – China’s heavy hand
- Australia bans Huawei gear – China cuts coal orders
- African Union HQ – Huawei gear sending daily reports to Shanghai
- US 23 Indictments Against Huawei – T-Mobile IP theft
Case Study: Huawei

“As a global company, Huawei is dedicated to closely collaborating, innovating and establishing international standards with other global organisations to ensure that the integrity and security of the networked solutions and services we provide meets or exceeds the needs of our customers and provides the assurance confidence required by their own customers.”

Case Study: Huawei

“Overall, the (UK) Oversight Board can only provide limited assurance that all risks to UK national security from Huawei’s involvement in the UK’s critical networks can be sufficiently mitigated long-term.”

UK Oversight Board Report to the National Security Advisor
March 2019
In early 2018, when asked by the Senate Armed Services Committee how the National Security Agency and the US Cyber Command were dealing with the most naked use of cyberpower against American democratic institutions, Adm Michael S. Rogers, then coming to the end of his term as commander of both organizations, admitted that neither President Obama nor President Trump had given him the authority to respond.

*Putin, Rogers said, “has clearly come to the conclusion that there’s little price to pay here and that therefore ‘I can continue this activity.’”*

“The Perfect Weapon” by David Sanger
Going Forward – “Release the EO!”

• Ideally, an EO would be part of a larger strategy for managing risk with the next generation of network technologies. The elements of a strategy should include:

• Close partnerships with the countries that share the assessment of the risk of using Huawei and the need to act to address it.

• Robust security standards for telecommunications equipment and supply chains (noting that some European customers of Huawei may try to dilute standards to ensure that Huawei has continued access to their markets).

• Foreign assistance to encourage developing countries not to buy Huawei. We will not match Chinese subsidies, but we can reduce the financial burden of a ban.

• Support for Western telecom infrastructure companies for research and development.
Prescription for an Executive Order

• Research on how to securely communicate over international networks that contain Huawei equipment, since many African and Middle Eastern companies already use Huawei.

• Formal bans (either complete or partial) on the purchase and use of Huawei technology.

• An EO on telecom supply chain security that clearly lays out U.S. policy.

• A long-term engagement strategy with China to bring its behavior into conformity with international norms for trade and security. China is not going away. It will always be powerful and the United States, working with its partners, must encourage and require change.

James Andrew Lewis, Center for Strategic and International Studies
International Cybersecurity Norms

• UN proposed treaty to limit the use of cyber attack and cyber weapons – 1998

• Distrust made efforts unworkable but led to effort for ‘confidence building’ and nonbinding measures

• 2010 report of the 2nd UN Group of Governmental Experts in the field of Telecommunications in the Context of International Security (UN GGE)

• Building “Norms”
Working Toward International Consensus

• 2013 GGE identified foundational norms that embedded cybersecurity in the existing framework of international relations and law.

  • the applicability of the principles of state sovereignty to cyberspace;
  • the centrality of international law and the UN Charter for governing state behavior; and
  • the need to respect the rights set forth in the Universal Declaration of Human Rights and other international instruments.
Where Are We?

• Cyber Agreements
  • Pause button
  • Effectiveness, compliance?

• Geo Political Competition
  • China and Russia (and US) will continue to use Cyber when in their own interests
  • Other players
Thank You

- Back up your data
- Don’t open suspicious email attachments
- Use VPNs in public WiFi spaces (or don’t connect)