Cybersecurity Policy and Planning:

Technologies for Keeping the Nation Safe

Dr. Abraham Wagner

June 5, 2019

arw@terrorstudies.org

Briefing Overview

- **The policy context – deterrence, and cybersecurity as a mission area**
- **Prior issues in cybersecurity**
- **National policy goals for cybersecurity**
- **Deterring cyber attack**
- **Transition from research to operations**

Complete discussion is in the study

This has been a team effort

Initial Comments – Impact of the Digital Revolution

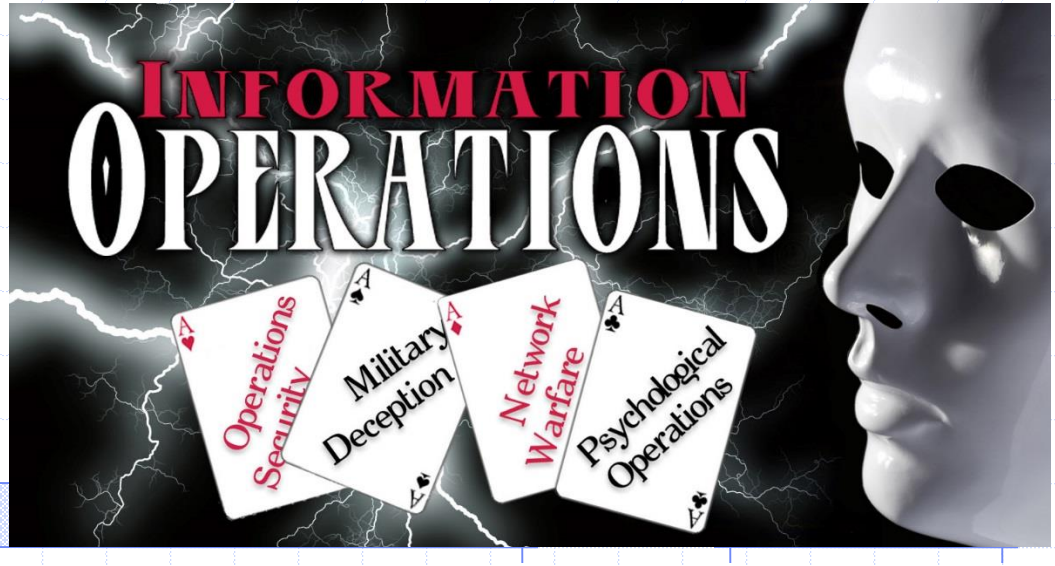
- **New world – Digital data has replaced analog files**
  - *Antiquated and physical media increasingly gone*
  - *World's comms and IT are part of a connected world*
- **World now dependent on Internet infrastructure**
  - *Never anticipated by government or private sector*
  - *Speed of revolution and challenges not anticipated*
  - *Biggest paradigm change since Guttenberg (15th Century)*
  - *Almost entirely commercial infrastructure*
- **Cybersecurity never kept pace**
  - *Many reasons – 1990s were a "lost decade"*
  - *Government and industry all at fault*

Traditional Cybersecurity Challenges

- **Denial of service, disruption of operations**
  - *Servers, systems, net-connected devices*
  - *Impair critical infrastructure operations*
  - *Destruction of systems and software*
- **Theft of data**
  - *Criminal activity, espionage, national security, others*
  - *Use by other-than-lawful owner of the data*

Information Operations – The Weaponization of Information

- **Malevolent use of Internet and social media**
  - *Largely through false or fake data*
- **Uses range from politics to terrorism**
- **Information warfare**
- **Technology enables IO at lightening speed and low cost**



The Policy Context: Deterrence and Cybersecurity as a Mission Area

Role of Deterrence

- **Recent policy guidance**
  - *National Security Strategy (December 2017)*
  - *National Defense Strategy (January 2018)*
  - *Nuclear Policy Review (February 2018)*
- **Need for "extended deterrence"**
  - *Also called "tailored deterrence"*
  - *Nuclear standoff with Russia, China, others*
  - *Cyberattacks and cyber weapons now in warfare domain*
- **No consensus yet on policy applying deterrence to threat of cyberwarfare**
  - *Threats of retaliation or other means?*
  - *National policy still in a state of evolution*

Continuity with Crime, Espionage and Cyberwarfare

- **Hard to distinguish cyberwarfare and cyber espionage prior to onset of conflict**
  - *Different from conventional and nuclear warfare*
  - *Very clear when "nuclear threshold " is passed*
- **Actions may begin as clandestine ops**
  - *Damaging attacks equivalent to military operations*
  - *Hostile network entry; denial of service; info ops*
  - *Same impact on infrastructure as military attack*
- **Need options for "peacetime" responses**
  - *Think differently about deterrence and tailored responses*

Attack Identification and Attribution

- **Nuclear detonation is immediately obvious**
  - *Generally clear who attacker is*
  - *Trackable delivery system or radionuclide fingerprints*
- **Different with cyberattack**
  - *Accurate and timely attack attribution may be problematic*
  - *Obfuscation possible with various techniques*
  - *Use of proxies or aligned groups*
- **May need to protect intel sources and methods**
  - *Could preclude overt response*
  - *May require covert response – communicated in advance for deterrent effect*

Variable and Uncertain Precision in Cyber Targeting

- **Cyberattacks may escape beyond original targets**
  - *Both attacker and responder affected*
  - *More widespread damage than anticipated*
- **Different from conventional attack**
  - *Conventional attacks would be clear acts of war*
  - *But damage may be far greater from cyberattack*
- **What are appropriate targets for response?**
  - *Response calibrated to intended or actual effects?*
  - *Were initial targets actually authorized?*
  - *Major issues of proportionality and escalatory dynamics*
  - *Impact on future ops and robustness of deterrence*

Asymmetries in Digital Vulnerability

- **U.S. benefits more from cyber technology than most potential adversaries**
  - *Creates asymmetric "cyber dependence"*
  - *Corresponding asymmetric "cyber vulnerability"*
- **U.S. economy and military rely on Internet**
  - *Almost total reliance on commercial infrastructure*
  - *Larger "attack surface"*
- **Increased vulnerability to catastrophic attack**
  - *U.S. may have far better cyber defenses*
  - *Need for individualized and detailed net assessments*

Cybersecurity as a Mission Area

- **Cyber deterrence presents more complex issues than nuclear or conventional military deterrence**
  - *Far fewer bright lines*
  - *More ambiguity between acceptable and unacceptable behavior*
- **Cyber operations, unlike nuclear, authorized under both Title 50 (intelligence) and Title 10 (military authorities)**
- **Cyberattacks on networked systems supporting military and national security**
  - *Potential for debilitating effects at very low cost*
  - *Degree of deniability*
  - *Deterrence must prevail over hostile threats*

Prior Issues in Cybersecurity

Rapid Evolution of Cyberspace

- **Concurrent merger of several revolutions never imagined or anticipated**
  - *IP and related Internet protocols*
  - *Communications technologies*
  - *Media revolution – social media and everything else*
- **ARPAnet showed utility of packet switching**
  - *New communications technologies increased bandwidth*
  - *Development in computer hardware and networking*
  - *Proliferation of systems and networks*
- **Nature of data transformed and connected world**
  - *Era of "big data" – world moves from analog to digital*
  - *Key sectors become dependent on net infrastructure*

Prior Issues in Cybersecurity

- **Major threats were largely ignored**
  - *Systems supporting national security and other critical sectors vulnerable to cyberattack*
  - *Threats not seen as great*
- **Internet is inherently vulnerable**
  - *Still operating on protocols from the 1960s*
  - *Inadequate for role Internet plays in 21st century*
  - *1990s were a lost decade for cybersecurity*
- **Earlier policy came without adequate resources**
  - *PDD/NSC-63; PPD/20; PPD/21 and PPD/41 failed to assign key cyber missions to agencies that could perform them or provide needed resources*

Prior Issues in Cybersecurity *(con't)*

- **Corporations did not develop secure systems**
  - *National policy based on idea that private sector would see the problem and fix it was wrong*
  - *Idea was that "the market" would respond to demands for privacy and security – never happened*
- **Government did not partner with industry**
  - *Needed key partnerships with technology and other sectors*
  - *Funded programs; data sharing; security clearances*
  - *Otherwise doomed to failure*
- **Existing statutes inadequate**
  - *Laws written before and during Cold War*
  - *Not sufficient for realities of cyberwarfare and cybersecurity*

Strategic Information Operations Ignored

- **Most cybersecurity efforts have been defensive**
  - *Denial of service, destruction, impairment, malware, theft*
- **Major issue now is use of Internet and social media for information operations**
  - *Politics, terrorism, geopolitical warfare*
- **Modern media provide opportunity for manipulation of opinion**
  - *Targeting of messages*
  - *Threats will only worsen in the future*
  - *"Deep fake" technologies and "tech tyranny"*

National Policy Goals for Cybersecurity

Actors and The Legal Regime

- **Cybersecurity embraces a larger set of actors than kinetic warfare and intelligence**
  - *Not a traditional national security problem*
- **Legal foundation for national security**
  - *National Security Act of 1947*
  - *Executive Order 12333 (1981)*
  - *Homeland Security Act of 2002*
  - *Intelligence Reform and Terrorist Prevention Act of 2004*
- **Cybersecurity remains in need of a defined organizational process**
  - *Analog to Executive Order 12333*
  - *Define specific agency roles and missions*
  - *Coordination of analytic, research and operations resources*

National Policy Goals

- **Meeting the challenge of cyber conflict**
  - *Major role cyber plays in any future conflict*
  - *Need portfolio of programs and operational capabilities*
  - *Able to deter cyberattack by potential adversaries*
- **Securing critical infrastructure**
  - *Critical sectors highly dependent on commercial infrastructure*
  - *Existing protocols inadequate and vulnerable*
  - *Need network architecture to meet current challenges*
- **Building a cyber workforce**
  - *Current shortage is about 300,000*
  - *Need an approach similar to "space race" of 1960s*
    - DARPA, NASA, NSF, National Defense Education Act, etc.

National Policy Goals *(con't)*

- **Building a partnership with industry**
  - *Technology sector, financial sector, others*
  - *DARPA started in 1960s but must be far greater*
  - *Compare to what IC did in other critical areas*
- **Creating a responsive security system**
  - *Industry, law enforcement and others need timely access to cyber data*
  - *Threat data needs to be shared – not a one way street*
  - *Much TS/SCI level data can be downgraded to Secret*
  - *Build a Secret level secure network for data sharing*

National Policy Goals *(con't)*

- **Repairing the vulnerabilities equities process**
  - *VEP determines whether or not to disclose info on new vulnerabilities – s/w developer can fix problem*
  - *Government can withhold info for intel and exploitation*
- **Approach Internet governance with realism**
  - *Field invented by lawyers and diplomats*
  - *Addresses problems that are real and imagined*
  - *Conflates management of technical resources with content behavior*
  - *Preserve values and opportunities essential to the Internet*
  - *No government owns, runs or controls the Internet*

National Policy Goals *(con't)*

- **Reforming export controls to serve U.S. interests**
  - *Technology supremacy challenged by China and others*
  - *Aggressive export controls no longer effective*
  - *Avoid agreements that are adverse to U.S.*
- **Recognize that the world is "going dark"**
  - *Devices/apps using encryption to meet user demands for privacy and security*
  - *Technology path cannot be stopped*
  - *Legislation doomed to failure – worldwide phenomenon*
  - *Technical programs must meet this reality*

National Policy Goals *(con't)*

- **Protect digital privacy and intellectual property**
  - *Increasing hacks and theft of data*
  - *Legitimate surveillance programs*
  - *Commercial use and misuse of "private" data*
  - *All areas of growing concern in U.S. and elsewhere*
  - *Legal regime is still evolving*
  - *Major differences with European nations*
  - *U.S. cannot permit other nations (China) to steal IP*
  - *Increase security against theft of IP with cyber attack*

Deterring Cyber Attack

Deterring Cyber Attack

- **Threat of retaliation is not a silver bullet**
  - *Reduce cyber vulnerability and improve resilience*
  - *Deterrence relies on enemy cost-benefit calculation*
- **Improve resilience by mitigating vulnerabilities**
  - *Eliminate unnecessary complexity*
  - *Reduce brittleness of IT systems*
- **Characterize adversary capabilities**
  - *Capabilities for active defense*
  - *Preemption using cyber tools*
  - *Support with kinetic attacks – comm nodes and lines*

Reducing Vulnerability with Defense

- **Securing entry points**
  - *Critical infrastructure shares Internet vulnerability and common entry points*
- **Mapping systemic vulnerabilities**
  - *Important for meeting challenge of disruption*
  - *Operate through disruption and reconstitution*
  - *Natural disasters and physical attacks*
- **Monitoring of specific threats**
  - *Combined with active and preferential defenses*
- **Strategic, operational and tactical intelligence**
  - *Needed for defense and offensive cyber*

Cyber Deterrence and Dissuasion

- **Tailored deterrence campaigns**
  - *Deterrence "tailored" to specific decision makers*
  - *Affects cost-benefit calculations on whether to attack*
  - *Different adversaries have different interests*
  - *China is in far different position vis-à-vis the U.S. than DPRK*
- **Different leaders process information differently**
  - *Similar to other deterrence domains, but*
  - *Cyber is different – given low-cost and attribution issues*
- **No government-wide or international agreement**
  - *Types of cyber intrusion are accepted or cause for response*
  - *"Playbooks" for cyber and non-cyber actions*
  - *Signaled and actual retaliation*

Key Technology Areas

- **Threat characterization**
  - *More accurate and timely intelligence*
  - *Cyber attack and intrusion capabilities*
- **Timely and accurate attribution**
  - *More rapid and certain attribution*
  - *Public attribution without compromise of sources/methods*
- **Signaling to adversaries**
  - *Embedded exploits and hostile code in adversary systems*
  - *Threaten assets important to leadership*
- **Targeting specific persons**
  - *Persons involved in cyberespionage, attacks*
  - *Target bank accounts, personal data, use dissuasive messages*

Cyber Vigilantes – Non-Governmental Approach

- **Enable victims of cyber attack to hack back**
  - *Illegal under 1986 Computer Fraud and Abuse Act*
  - *Deters those from entering field*
- **Time to change the law?**
  - *Raise the costs for potential hackers*
  - *Broader range of retaliatory actions*
- **Vigilantes have been anathema to legal regime**
  - *Reasons are obvious and subject to prosecution*
  - *Useful where law has been dysfunctional or non-existent*
  - *"Wild West" analogy often use with cybersecurity*

Resilient Cyber Infrastructure

- **Dramatically increase resilience of infrastructure**
  - *Detect malicious cyber activity*
  - *Automated remediation and response to cyberattack*
  - *Software tools to make network and devices more secure*
- **Resilient networks – fight DDoS attacks**
  - *Dispersed Computing Program*
  - *Extreme DDoS Defense (XD3)*
  - *EdgeCT*
- **Assured engineering – protect embedded systems**
  - *High-Assurance Cyber Military Systems (HACMS)*
  - *Cyber Assured Systems Engineering (CASE)*

Resilient Cyber Infrastructure *(con't)*

- **Eliminating vulnerability in algorithms**
  - *Space/Time Analysis for Cybersecurity (STAC)*
- **Automated repair and adaptation of software**
  - *Mining and Understanding Software Enclaves (MUSE)*
  - *Building Resource Adaptive Software Systems (BRASS)*
- **Code obfuscation – "security through obscurity"**
  - *Safeware*
- **Sensing and detecting malicious behavior**
  - *Vetting Commodity IT Software and Firmware (VET)*

Resilient Cyber Infrastructure *(con't)*

- **Automated vulnerability remediation**
  - *Cyber Grand Challenge (CGC)*
  - *Computers and Humans Exploring Software Security (CHESS)*
- **Binary resilience**
  - *Cyber Fault-tolerant Attack Recovery (CFAR)*
- **Critical infrastructure rapid recovery**
  - *Rapid Attack Detection, Isolation and Characterization Systems (RADICS)*
- **Internet of things protection using the analog domain**
  - *Leveraging the Analog Domain for Security (LADS)*

Resilient Cyber Infrastructure *(con't)*

- **Data integrity**
  - *Media Forensics (MediFor)*
- **Data privacy**
  - *Private data used only for intended purpose – BRANDEIS*
- **Configuration security**
  - *Configuration Security (ConSec)*

Broad Cyber Situational Awareness

- **Rapid and accurate cyberattack warning**
  - *Track perpetrator in specific systems and hosts*
- **Behavior and threat detection**
  - *Adjustments to network and host sensors at machine speed*
  - *Wireless Network Defense*
  - *Cyber-Hunting at Scale (CHASE)*
- **Enhanced attribution**
  - *Enhanced Attribution (EA)*
- **Tracking adversary actions within hosts**
  - *Transparent Computing (TC)*

Accurate and Robust Cyber Response

- **Collaborative planning and execution**
  - *Foundational cyberwarfare program – Plan X*
    - Platforms for DoD to plan and assess cyberwarfare similar to kinetic warfare
- **Social engineering defense**
  - *Active Social Engineering Defense (ASED)*
- **Gray space operations**
  - *Majority of botnets exist in "neutral" networks – "gray space"*
  - *Harnessing Autonomy for Countering Cyberadversary Systems (HACCS)*

Transition to an Inherently Secure Internet

- **ARPAnet / Internet never designed for security**
  - *Antiquated protocols and technologies still in use*
  - *Decades of "band aids" and patches that don't work*
- **Privacy/autonomy interests at odds with strong authentication/identification**
  - *Need to resolve basic conflict for inherently secure Internet*
- **Also think about vulnerability of infrastructure**
  - *Commercial cables, servers, hosts, not protected*
  - *Example – 13 "root routers" in U.S. all in commercial buildings*
    - Unguarded – 13 terrorists could blow them away simultaneously
    - No plan or equipment to replace them - Internet in U.S. wiped out

Transition to an Inherently Secure Internet *(con't)*

- **Debate over what is possible and how to do it**
  - *Start with "islands" – strong authentication/limited access?*
  - *Islands with strong encryption and secure enclaves?*
    - Protect terminal computers and connected devices
    - Control user access to prevent migration
- **Non-secure and secure networks may co-exist**
  - *User access from same terminal?*
    - Need to prevent migration (prior examples exist in IC)
- **Concept for heterogenous Internet**
  - *Robust authentication and identification*
  - *Gaps between autonomous and secure portions*
  - *Protection against insider threats*

Transition from Research to Operations

Integrating Defensive and Offensive Cyber Operations

- **Current policy recognizes major role of cyber in any future conflict**

  Space and Cyberspace as Warfighting Domains: The Department will prioritize investments in resilience, reconstitution and operations to assure our space capabilities. We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations (DoD 2018 National Defense Strategy)

- **National policy still based on deterrence model**
  - *Portfolio of defensive strategies*
  - *Ability to conduct offensive operations when needed*
  - *Capabilities to deter attacks by potential adversaries*
    - Concept of "tailored deterrence" - *2018 Nuclear Posture Review*
    - Authorities under both Title 10 and Title 50

Proactive Cyber Defense

- **DoD responsible for defending U.S. from strategic cyberattack?**
  - *Collateral role of DHS and others?*
  - *Most current PDs and EOs are wrong and confusing*
- **Need for "stress testing" against threats**
  - *Also known as "white hat hacking," "red teaming," etc.*
  - *Requires imaginative approach to deal with real cyberattack*
  - *Similar to testing of other key warning systems*
- **Program could include**
  - *Facilities identified as "critical infrastructure"*
  - *Mapping Internet attack routes and installing countermeasures*
  - *Targeting hostile computers in advance*

Competing in the Information War

- **IC recognizes growing threat from hostile info ops**
  - *Politics, terrorism, geopolitical warfare etc.*
  - *People in modern world dependent on connected devices*
    - Susceptible to both mass and individualized manipulation
- **Most cybersecurity efforts are defensive – not focused on malicious and malevolent use**
  - *Infrastructure used to influence/manipulate entire populations*
  - *Competing with Russia and others requires other technologies*
  - *New field of "cognitive security"*
- **Need to consider key questions**
  - *Roadblocks from current laws, policies, authorities?*
  - *Organizational structure to manage national effort?*

Final Thoughts – A New Foundation for Cybersecurity

- **Rethink agency roles, missions and legal authorities**
  - *Trend of last 30 years needs to be reversed*
  - *U.S. has major technical and societal advantage*
  - *Can be harnessed if right steps are taken*
  - *Compare to problems of the IC in the 1970s*
- **Repeated high-levels studies identified the problems but never fixed them**
  - *Agency roles and missions not properly assigned*
  - *Adequate federal resources never provided*
    - Assumption that industry would "fix" the problems was in error. It is a classic "public goods" problem

Final Thoughts – Information War

- **We are now losing the information war**
  - *Law prohibits serious action*
    - 50 USC §3093(f) and 1974 Privacy Act
  - *2017 Defense Authorization Act empowers DoD and State*
    - State Department (GEC) lacks technical resources and funding
    - Information warfare is warfare – not a State Department mission
- **Serious response requires serious programs**
  - *Still need to resolve "roles and missions" issue for cyber*
  - *Programs will be in DoD and the Intelligence Community*
  - *Our best and brightest not working on it now*
- **May take major disaster before we get serious**
  - *Awareness growing but not fast enough*

Final Thoughts – A New Foundation for Cybersecurity

- **Cybersecurity landscape is uniquely dynamic and complex**
  - *Rate of underlying technological change*
  - *Unevenness of hardware and software adoption*
  - *Low barriers to entry*
  - *Large number of existing and potential actors*
  - *National security and domestic policy can't be separated*
- **Realistic approach must deal with this complexity**
  - *Create technological, legal and organizational foundations that work – respond to changing threats and technologies*
  - *Not enough to respond to today's threats*

Study Team

David Aitel
Immunity, Inc.

Sophia d'Antoine
Center for Advanced Studies on Terrorism

Edward Doyle
Center for Advanced Studies on Terrorism

Daniel Gallington
Center for Advanced Studies on Terrorism

Thomas Garwin
Center for Advanced Studies on Terrorism

Daniel Guido
Trail of Bits, Inc.

Nicholas Rostow
Yale Law School

Daniel Gallington
Center for Advanced Studies on Terrorism

Ryan Stortz
Trail of Bits, Inc.

Abraham Wagner
Columbia Law School

Lisa Wiswell
Center for Advanced Studies on Terrorism

RESEARCH ASSISTANTS

Baruch Bacharach
Columbia Law School

Christine Chen
Columbia Law School

Theodore Rostow
Yale Law School

Kathryn Witchger
Columbia Law School