Cyber Power: Fundamentals and Beyond

Dr. Srijith Nair
srijith@srijith.net

Public Release Notice

This presentation was delivered at a
closed-door session of
The Takshashila Institution
In 2018

Released to public on 03 Aug 2020

Caveats

I am not a policy wonk, I am a technologist with interest in strategy and policy

I use a “power”-tinted view of cyber domain

Views expressed here are my own and not that of my past, current nor future employers

Outline

1. Concepts Walkthrough
2. Cyber Characteristics
3. Privacy, Freedom in Cyber
4. Beyond Cyber - IW
5. Going Dark
6. Getting a Grip
7. India and Cyber

Power

Power is the ability to influence others to obtain the outcomes one wants through

- hard power behavior (coercion and payments) and
- soft power behavior (framing agendas, attraction and persuasion)

- Joseph S. Nye, Jr.

Cyber space

- Typical use of ‘cyber’ is as a prefix that stands in for electronic and computer related activities
- Cyberspace constituted by layers of activities

Layers	Economic laws	Political laws
Physical	rival resources, increasing marginal costs	sovereign jurisdiction and control
Informational (virtual)	increasing returns to scale	practices that make jurisdictional control difficult

Cyber power

is “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.”

- Daniel T. Kuehl

Domains of power

- 4 traditional (natural) domains:
  - Air
  - Water
  - Land
  - Space
- Cyber: 5th domain
  - man made
  - recent
  - fastest rate of technological development

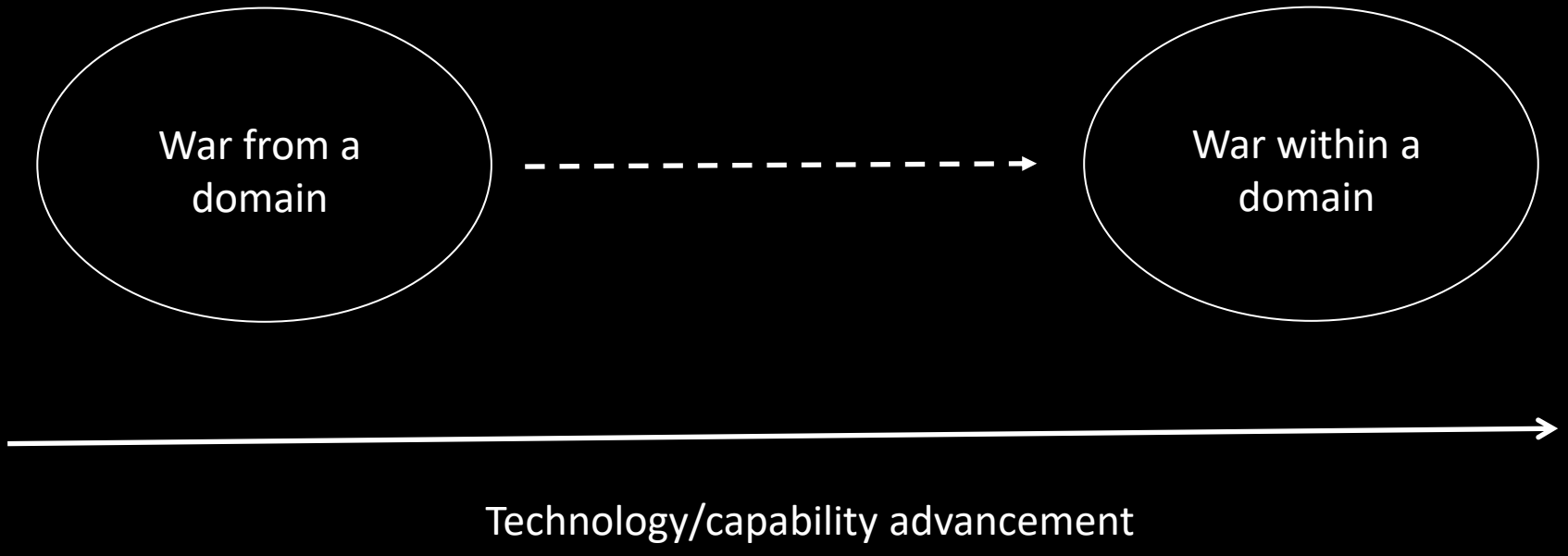
Cyber and Land

cyber shares three characteristics with land warfare – though in even greater dimensions: the number of players, ease of entry, and opportunity for concealment...On land, dominance is not a readily achievable criterion.

- Franklin Kramer

(though “take and hold” doesn’t make sense in cyber, much like in air, space)

War *from* → War *within* a domain



War *from* cyber domain

- use of cyber to sense, plan, direct and strike from
- attack occurs in physical domains
- captured by “network-centric warfare” concept
- promise to lift Clausewitzian “fog of uncertainty”

e.g. Dispatching cyber-controlled UAV using networked sensors and geospatial info to fire a weapon on an enemy target

War *within* cyber domain

- In some way as old as domain ('hacking')
- Aims to manipulate information
  - integrity (modification of information)
  - confidentiality (disclosure of information)
  - availability (availability of information)
- All attacks are not equal
  - Crime
  - Espionage
  - War (Disrupt, deny, degrade, destroy, or deceive as per UAF)
  - Tools, techniques, procedures are often the same, difference mostly being on the objective, effect

FORCE, VIOLENCE, WAR

War is “an act of force to compel our enemy to do our will”

“Force – that is physical force, for moral force has no existence save as expressed in the State and the law – is thus the means of war.”

Carl von Clausewitz

Cyber and violence

- Conflict from cyber domain can be violent
- Conflict within cyber domain is non-violent
- Clausewitz's definition of war easily applies to conflicts within cyber domain
- What about Clausewitz's definition of ***force***?
- Definition needs to expand beyond 'physical'
- Within cyber, 'force' is about 'power to hurt'

‘War’
What does it mean for Indian armed forces?

The U.S. has affirmed that the International Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace.

- General Keith Alexander

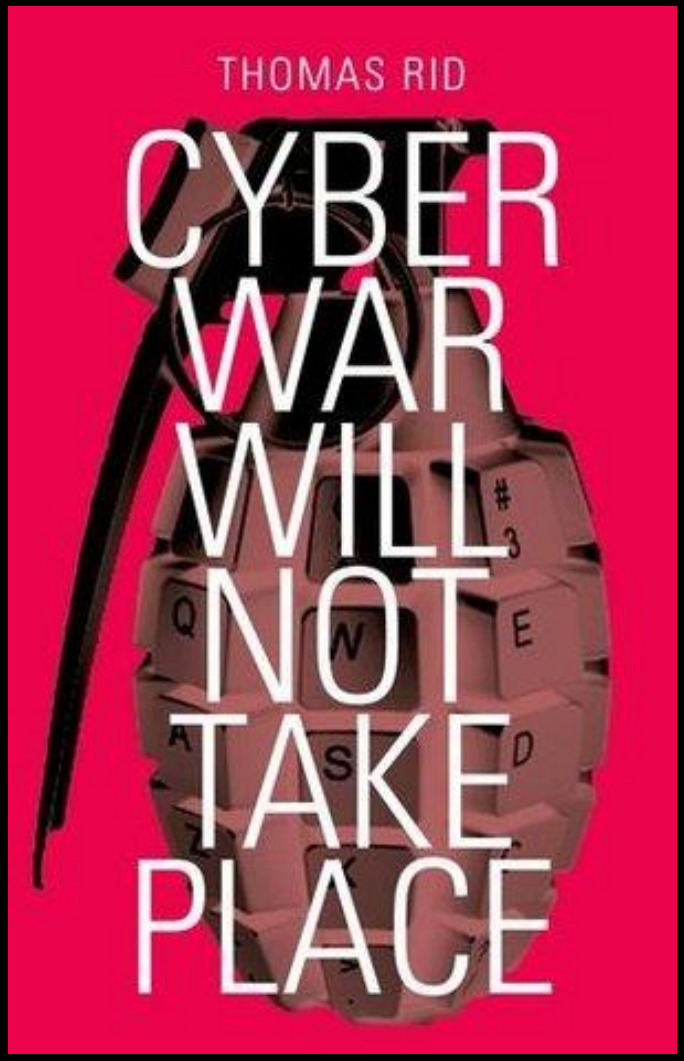
Cyber “War”?

- US has officially classified cyberspace as a ‘warfighting domain’. Several nation states have followed suit, officially or otherwise.
- Betting against technological power (and its advancement) is never a winning strategy
- War will anyway be unlikely to be fought purely within cyber

Cyber “War”?

Maybe it is this difficulty to call cyber attacks “wars” that make it “anybody’s game”

- John Arquilla


THOMAS RID
CYBER WAR WILL NOT TAKE PLACE

POWER DIFFUSION

Actors

- Cyber instruments are a great leveler
- Cost of acquiring instruments are low
- Impact derived from low cost instruments
- States actors
- Non-state actors
  - Organizations and structured networks
  - Individuals and lightly structured networks
  - Proxy players/agents

"On the Internet, nobody knows you're a dog."

Power diffusion

- Cyber domain has extreme power diffusion
- Evident from
  - large number of actors
  - reduction of power difference across them

Powerful nations have greater resources, but also bigger vulnerabilities – leading to offense being preferred over defense

Power diffusion

On the Internet, all dogs are not equal.

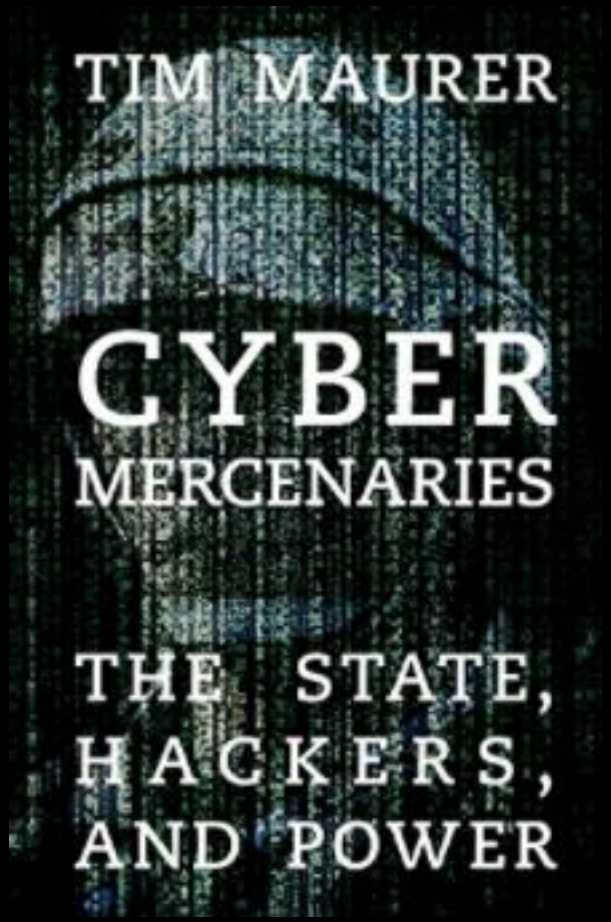
Power diffusion ≠ power equalization

“ (…) smaller dogs still bite, and dealing with those bites can lead to a complex politics.”

- Joseph S. Nye, Jr.

Big and Small

- Small actors face bigger response from stronger power
- Other instruments of power, in other domain is very relevant
- Retaliation outside cyber is an open option
- Consider the US position



Don’t be dissuaded by the cover ☺

Explores the unique cyber domain actor landscape of proxies in cyber attacks.

Helps to understand and manage the impact and risks of cyber proxies on global politics.

TEMPO

Speed of light

- Operations within cyber is near-instantaneous
- Controls and commands from cyber as well
- ‘OODA loop’ approach lacks applicability
- Offense out-tempos defense
- Technological advances may provide us some tools to bring back OODA loop back
- Intelligence, analysis becomes important
- Clausewitz’s “friction” becomes very important

In the fog of war, what is our tolerance for uncertainty, especially given the inherent tempo of “actions of war” within and from cyber?

Managing cyber war

Cyber attacks can be managed through

- deterrence
- offensive capabilities
- defense
- resilience

What part does defense play in cyber war?

Works on nuclear war doctrine might help, but will it boil down to deterrence?

Vectors / Targets

- Vectors
  - Kinetic
  - Electromagnetic
  - Cyber
- Targets
  - Governmental
  - Military
  - Civilian

NUCLEAR, CYBER & DETERRENCE

Cyber vs. Nuclear

- Similarities:
  - short delivery time
  - very hard to defend against
  - only most technically competent states seem to be able to use it as a weapon

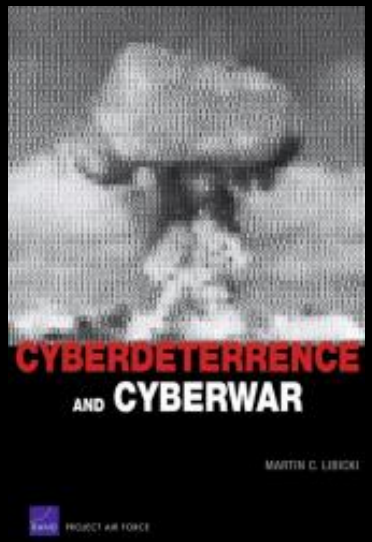
- Logical to use nuclear deterrence principles as guide to develop cyber deterrence

Cyber vs. Nuclear

- However
  - Cyber attacks lack the catastrophic dimensions
    - destructiveness of single weapon
    - ***assuredness*** of that destruction
    - lack of visible output, centered around speculations
  - Adjunct rather than overwhelming weapon
  - Lack of broad debate over use of such weapons
  - Hard to do attribution
  - Inability to re-use weapons

Pre-delegation Policy

- “Always/never dilemma” of nuclear
  - Always be ready, never be used without authority
- Led to pre-delegation of use authority
  - delineated procedures authorizing when and how weapons could be used by tactical commanders
- Pre-delegated → automated authority?
- Pros and cons exists, as always, including that which touches on civilian liberties



Cyberdeterrence and Cyberwar
- Martin C. Libicki

Do we know who did it?
Can we hold their assets at risk?
Can we do so repeatedly?
If retaliation does not deter, can it at least disarm?
Does retaliation send the right message?
Do we have a threshold for response?
Can we avoid escalation?
What is attacker has little worth hitting?

One time use of cyber weapons

- Distinguishing aspect of cyber instruments
- Antidote (patch, update) available soon
- Make attacks harder to reuse, more precious
- 0-day attacks becomes sought after, horded
- Ethics of state actors hording, buying vul.
- Big market around vul., high stakes
- Indian agencies known to buy vul. in market
- Not a taboo like weapons in other domains

Attribution

- Attribution is hard in cyber domain
- Proxy actors complicate matter further
- Interestingly, when stakes are high, certainty need not be 100%!
- Recent attributions to Russian (non?) state actors is an indication of things to come
- False-flag operations aim to undermine confidence in attribution process
- Technology will also improve in the area

Side note: Global common or common pool resource?

- Cyber domain is often described as public good / global common i.e. from which all can benefit, and none can be excluded
- Ignores physical layer/infra
  - scares resource
  - under control of states

"common pool resource" (Elinor Ostrom) from which exclusion is difficult and exploitation by one party can subtract value from other parties.

PRIVACY, FREEDOM IN CYBER

Cyber and Privacy

- Political legitimacy of government
- Global economic aspect of cyber
- Anonymity: enabler vs. anti-democratic effect
- Privacy safeguards
- Privacy vs. civil liberties
- India as a surveillance state
- Assuring citizens of the strategy, enforcing

“Less privacy does not automatically lead to less political freedom and fewer civil liberties if free speech and freedom of assembly are protected.”

- James A. Lewis

Cyber and Privacy

- Need for hybrid approach
  - Norms, laws, technologies to preserve privacy in some areas, constraint them in others
  - Maturity of the democratic institution is key
- Privacy means different in different societies
- Privacy incursions are tolerated/expected
- Unregulated cyber domain cuts both ways

Freedom *of* Internet

vs.

Freedom *via* Internet

Freedom vs. responsibility

- Easier to justify (extreme) measures under extreme circumstances
- But systemic curtailing of freedom erodes faith, transparency, legitimacy

BEYOND CYBER – INFORMATION WARFARE

Information warfare
More than cyber security

The sheer volume of the IRA's effort staggers the imagination. All told, it posted some 80,000 pieces of content in 2015, 2016, and 2017. Facebook has struggled to wrap its arms around the IRA's activities in the year since the election; according to Facebook's estimates, more than 126 million Americans saw some of the IRA's propaganda. The company estimates that the IRA spent around $100,000 to promote some 3,000 different ads related to the campaign, all part of what it says are about 470 "inauthentic accounts and Pages." On Twitter, the Russian efforts garnered more than 131,000 tweets, and there were more than 1,000 videos uploaded to YouTube.

Zuckerberg: Facebook is in 'arms race' with Russia

Facebook CEO Mark Zuckerberg has told US senators his company is in a constant battle with Russian operators seeking to exploit the social network.

"This is an arms race. They're going to keep getting better," he said.

Mr Zuckerberg was answering questions in the wake of the Cambridge Analytica data collection scandal.

Russian take on Cyber

- reflexive control: a process in which the controlling actor conveys to the target various motives, reasons that cause the latter to reach the decision sought by the controlling actor
- Reflexive control exploits moral, psychological, and other factors, as well as the personal characteristics of commanders.

Gerasimov Doctrine

“In the 21st century we have seen a tendency towards blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template

(…)

Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals”

- General Valery Gerasimov
  Chief of the general staff of Russia’s armed forces

Chinese take on cyber

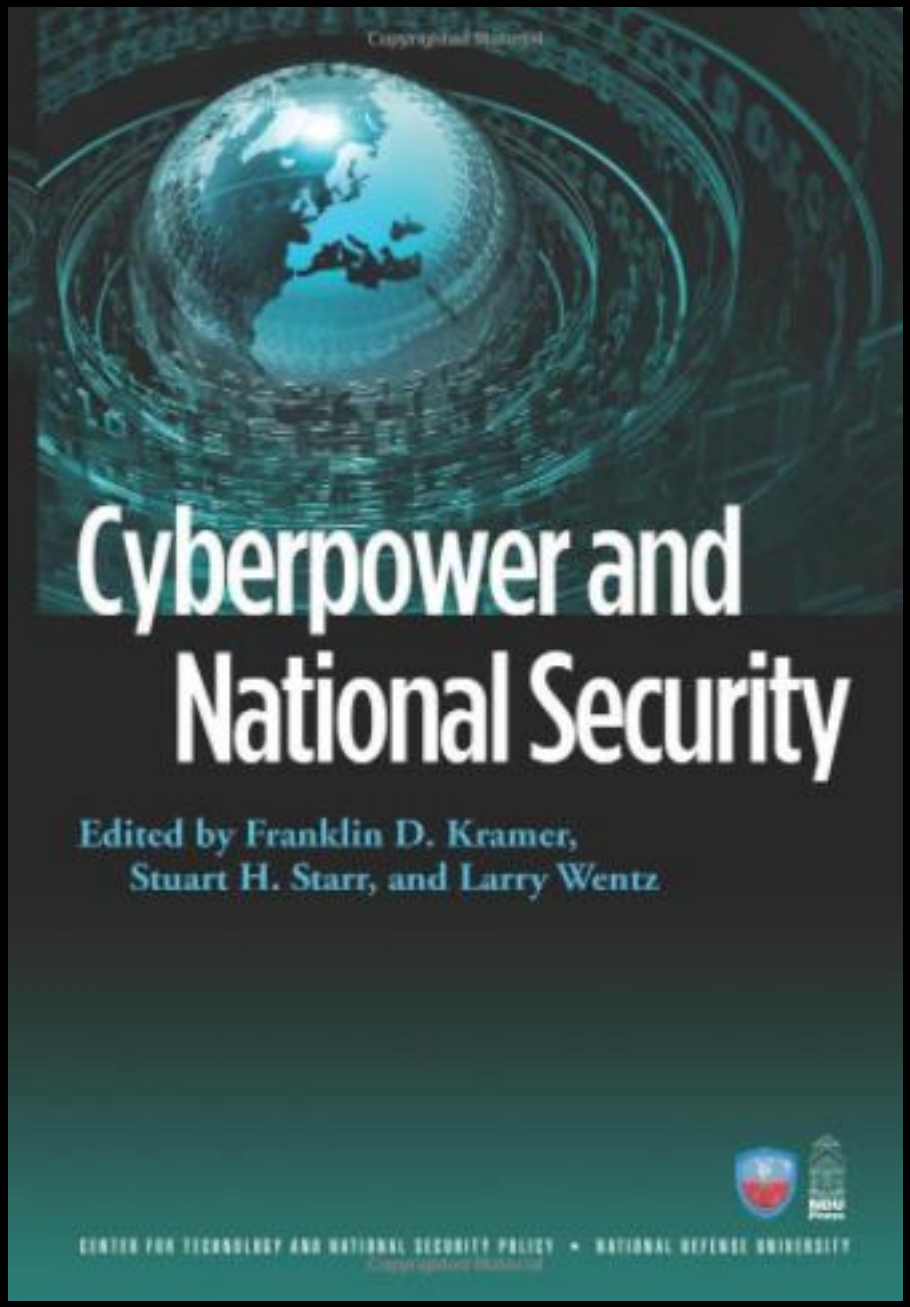
- ‘cyber’ as a word not common in strategy
- ‘informationization’ is typically employed

“struggle between opposing sides making use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology”

– 2007 China National Defense News definition of cyber warfare

Traditionally, Oriental people emphasize stratagems, and Occidental people emphasize technology. . . . Occidental soldiers would seek technological means when encountering a difficulty, while Oriental soldiers would seek to use stratagems to make up for technological deficiencies without changing the technological conditions.

- Niu Li, Li Jiangzhou, and Xu Dehui, “Planning and Application of Strategies of Information Operations in High-Tech Local War,” China Military Science


Cyberpower and National Security
Edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz
CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY • NATIONAL DEFENSE UNIVERSITY

GOING DARK
STRONG ENCRYPTION

“Going dark” debate

- Ubiquitous end-to-end encryption
- Enough alternatives to choose from
- Terrorism / national security vs. crime prevention
- “national security” fatigue
- Question statement. Is it really going dark?
- Lack of emperical evidence
- Introduces gaping security hole
- Cost > benefit given the underpinning of commerce, erosion of trust?

Keys under doormats: mandating insecurity by requiring government access to all data and communications

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J. Weitzner

Journal of Cybersecurity, Volume 1, Issue 1, 1 September 2015, Pages 69–79, https://doi.org/10.1093/cybsec/tyv009

Published: 17 November 2015 **Article history**

We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse "forward secrecy" design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.

Techniques overview

Circumvent Protections	Lawful Hacking (including surreptitious updates)	Brute Force			
Regulate Technology	Design Mandates	Weaken Standards	Regulate Sale/Use	Export Control	
Compel Assistance	Compel Provider Assistance	Compel User Decryption			
Employ Workarounds	Analyze Metadata	Exploit Sensor Data	Adapt Conventional Police Methods	Data Localization	Liability

From “Encryption Policy in Democratic Regimes”
https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf?dm_t=0,0,0,0,0

When crypto is outlawed, only outlaws will have crypto.

- Phil Zimmerman

Levels of attacks

- Levels of attacks
  - Crime, theft
  - Espionage
  - War
  - Terrorism
- Economic impact of cyber crime, IP theft
- Lot of policy work focuses on ‘war’ (cool?) while espionage and theft/crime is often ignored / after-thought
- Espionage – national, civilian and corporate level

Improving Cyber Security - Approaches

- Traditional
  - Technical: newer design, better response
  - Criminal: law enforcement against crime
  - Warfare: military approach to conflict
- Newer
  - Public Health: bio-disease analogy, stop spread
  - Environmental: grassroots societal approach to pollution
  - Irregular warfare: winning heart & mind, anti-insurgency

Improving Cyber Security - Traditional

	Technical	Criminal	Warfare
Viewpoint	Non-state actors should improve technology and response for the best defenses	States should improve defenses by using law enforcement to stop non-state criminals	States should improve defenses for defeating states and non-state actors
Primary Role Belongs to Whom	Non-state actors who are extremely active in all aspects of this approach	Governments as law enforcers	Governments as warfighters
Generally How?	Enables non-state actors on defense	States lock up non-state cyber criminals	Improves state defenses and offenses
Specifically How?	Non-state actors lead in many kinds of cyber incident coordination, improved and secure technology, standards	States undertake forensics, improve laws; train cyber smart police, prosecutors and judges	States treat warfare in cyberspace as analogous to warfare in other domains

Improving Cyber Security - Newer

	Public Health	Environmental	Irregular warfare
Viewpoint	State and non-state actors improve defenses as if confronting pandemic threat	State and non-state actors could improve defenses if cyberspace is seen as polluted domain	Militaries could improve defenses if cyber conflict is seen as irregular warfare
Primary Role Belongs to Whom	Governments as cyber public health coordinators (e.g. cyber WHO or CDC)	Governments as law enforcers	Gov (as lawmaker, regulator) and non-state actors (as non-gov organizations, individuals)
Generally How?	Improving defenses in both states and non-states	Enrolling non-states and states to improve defenses	Improving state defenses against non-state offense
Specifically How?	International agreements to measure and share data, respond to incidents, enroll non-state actors	Creating norms of behavior, legal regimes based on "pollution" of	Change of mindset based on tenets and tactics of irregular warfare

Kill Chain and Cyber

- Military concept on structure of an attack:
  - target identification
  - force dispatch to target
  - decision and order to attack the target, and finally
  - destruction of the target
- Lockheed Martin adapted this to model intrusions into computer networks, system
- Meant to defend the computer systems

A: ADVANCED

Targeted, Coordinated, Purposeful

P: PERSISTENT

Month after Month, Year after Year

T: THREAT

Person(s) with Intent, Opportunity, and Capability

RECONNAISSANCE

Harvesting email addresses, conference information, etc.

DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

INSTALLATION

Installing malware on the asset

ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

Kill Chain in Cyber

- Helps define stages of cyber attacks
- Provides common terminology conventions
- Helps analysis of incidents
- Helps identify controls that did not work to prevent or detect

Kill Chain in Cyber

Defensible Actions:

- Detect: determine whether attacker is poking around
- Deny: prevent information disclosure and unauthorized access
- Disrupt: stop or change outbound traffic (to attacker)
- Degrade: counter-attack command and control
- Deceive: interfere with command and control
- Contain: network segmentation changes

Indian Cyber Domain State-of-art

- Consider scenario
  - Indian block effort to sell armory to Pakistan
  - Proxy actors bring down BSE, billions lost
- No clarity on thresholds for triggering ‘necessary and proportional’ response
- No stockpile of instruments to be able to confine attacks to within cyber domain, resulting in spillage into other domains

Indian Cyber Security Approach

1. National/domestic Internet Policy
   - Clarify authority and mandates of the various central, state agencies. Prevent turf war
   - Unified domestic-defense approach to cyber sec
   - Make full use of existing governance structures, creating new ones only when needed
   - Follow up and implement existing proposals!
   - Create strong criminal laws and enforcement structure for wrong doings in cyber domain

Indian Cyber Security Approach

2. Development of defensive/offensive capabilities, security posture
   - Central Cyber Command for military effort coordination?
   - Push for military, civilian, private co-ordination
   - Facilitate indigenous development and where necessary, the purchase of cyber capabilities
   - Articulate national security doctrine to guide their use

Indian Cyber Security Approach

3. International efforts, diplomacy
   - cyber by nature is global, so is problems, solutions
   - international security governance is crucial
   - various forms
     - bilateral agreements between nations
     - working groups composed of public, private, scholars
     - formal multilateral agreements on international policy
   - lead in IGOs, provide resources/funding for ITOs
   - help create non-proliferation regime to limit deployment of cyber and cyber-physical weapons

Notes on International Cyber Norms

- Steer clear of sanctions arrangement that targets emerging technologies, individuals & organisations in India who could develop them
- Work towards creating a new legal and political architecture around cyber and cyber-physical weapons
- Enter it as a manager and not exclusively as a subject, disaggregating any links with the extant nuclear non-proliferation regime

Notes on International Cyber Norms

- Norms need to be clear, utilitarian in nature
- Grafting norms on existing frameworks (e.g. human rights, laws of war), may bring more success
- Multipronged and multilevel approaches to norm dissemination
- Complementary implementation of law
- Funding and assistance to ‘do the right thing’

Indian Cyber Security Approach

4. Focus on defense
   - secure by design, secure engineering
   - help secure critical infrastructure, including standards and protocol implementation (e.g. BGP, DNSSec, IPSec, crypto primitives etc.)
   - improve software security at gov. level
   - re-orient public-private partnership on proactive security, building it baked in, using collective knowledge
   - incentivize secure dev. in civilian and corporate level
   - assert marketplayer clout to demand security hygiene

Indian Cyber Security Approach

5. Push for private sector involvement
   - make use of expertise, experience
     - early, exhaustive involvement in development of cyber
     - controls, operates, develops major infra, tech solution
     - protocol, content, service, defense development
     - in best practice refinement, enforcement
   - in public policy making
     - ensures relevancy, consistency of policies developed
     - sensible technological, market-relevant solutions

Critical Infrastructure protection in IN

6. Critical Infrastructure Protection
   - Classify critical-non critical infra, service gradient
     - Critical
       - Undersea cables
       - Governmental PKI infrastructure
       - Military networks
       - Private sector networks in finance, energy
   - Define, implement proportional defense
   - Define, implement escalation, response strategy

Indian Cyber Security Approach

7. Secure the weakest link – users
   - Informed user
   - Awareness campaign, security hygiene education
   - Need to know, need to operate principles
8. Lead by civilian agencies?
   - Corporate, civilian needs & issues are glossed over
   - Undue militarization of cyber domain
   - Military agency leading cyber defense reeks of conflict of interest (spycraft relies on deficiencies)

Notes on Undue focus on military

Cyber security is confluence of various issues

- military
- economic
- cultural
- diplomatic
- social

Ignoring rest and devoting focus on military aspects – the result of putting national security agencies in the lead – will result in a flawed approach

Indian Cyber Security Approach

9. Be good global citizen
   - Don’t approach cyber as war domain
   - Build an informed society
   - Be a responsible global player
   - Be a leader among global player

FIN