A BRAVE NEW WORLD:
Cyberworld Meets Cognitive Neuroscience & Public Policy

Prof. Birol Yesilada & Prof. Barbara Endicott-Popovsky

Mark O. Hatfield Center for Cybersecurity

NSA/DHS National Center of Academic Excellence in Cyber Research

Portland State UNIVERSITY

Evolution of the Threat

Accelerating Cyber threats forcing governments and industries to address their vulnerabilities

- Increased economic and reputational impact
- USG now openly identifying state-sponsored attacks
- Attacks moving from DDoS to destruction of assets Adversaries using Cyber as a military weapon

- U.S. federal agencies faced 31,107 cybersecurity incidents in 2018 (Source: 2018 FISMA report)
- Security breaches have increased by 67% since 2014 and 11% since 2018 (Source: Accenture)

APRIL 2007
ESTONIA

Denial of Service attack likely by **Russian activists** on the Estonian government

AUG 2008
GEORGIA

Hack on government computer networks likely by **Russian state actors** ahead of troop incursion

MARCH 2011
RSA

Nation state actors from China stole data related to RSA Secure tokens targeting defense secrets and related IP. **US replacement costs: $50M-$100M**

JAN 2010
GOOGLE

Hackers stole intellectual property and sought access to Gmail accounts; **the attack originated from China**

APRIL 2009
Lockheed JSF

JSF design and electronics systems files hacked by **China, which later produced the J20**

LATE 2014
YAHOO!

In late 2014 Yahoo! experienced one of the largest breaches in history, with over 500 million users information stolen in what is **believed to be a state-sponsored attack**

JUNE 2013
SNOWDEN

Edward Snowden **leaked up to 1.7 million classified files from the NSA** about the agency's surveillance programs

AUG 2012
SAUDI ARAMCO

DDOS attackers infected the hard drives of **over 30,000 computers**, effectively destroying data. US government officials suggest **Iranian regime was to blame**

JUNE 2015
OPM

The largest breach of federal employee data in recent years. **China accessed up to 22 million personnel records for espionage purposes**

JUNE 2015
SAUDI ARABIA, ISRAEL

Cyber espionage attacks against critical government systems by **Iranian threat actors**

NOV 2014
SONY

Attack against several internal data centers **(over 100TB of data)** delayed the release of *The Interview* – attributed to **North Korean state actors**

MAY 2017
WANNACRY

A worldwide ransomware campaign widely **attributed to North Korea** affects more than 200,000 computers in 150 countries

NOV 2018
AUSTAL

Australian shipbuilder Austal suffers a ransomware attack with company data, including some unclassified ship designs; **many news reports suggest Iran was behind the attack**

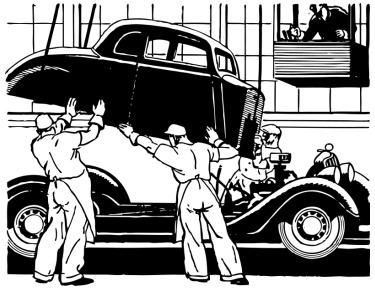
OCT 2016
DNC HACK

DHS and DNI name **Russia** responsible for **hacking the Democratic National Committee** to steal and disseminate over 20,000 emails

SEPT 2017
EQUIFAX

In Feb. 2020 the U.S. DOJ charged **4 Chinese** Army personnel for the hack which compromised the private data of 145 millions Americans

Humanity's Progression:
Where We've Been and Where We're Going



Microsoft Windows

1600-1825
Agricultural Age

1825-1980
Industrial Age

1980-NOW
Information Age
Phase I

NOW
Information Age
Phase II

The History of Cyber Conflict

Stages	Realization	Takeoff	Militarization
Timeframe	1980	1998–2003	2003–present
Dynamics	Attackers have advantage over defenders	Attackers have advantage over defenders	Attackers have advantage over defenders
Who Has Capabilities?	United States and few other superpowers	United States and Russia with many small actors	United States, Russia, China, and many more actors with substantial capabilities
Adversaries	Hackers	Hacktivists, patriot hackers, viruses, and worms	Neo-Hacktivists, espionage agents, malware, national militaries, spies, and their proxies, hacktivists
Major Incidents	Cuckoos Egg (1986), Morris Worm (1988), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Eligible Receiver, Solar Sunrise, Moonlight Maze, Allied Force, Chinese Patriot Hackers	Titan Rain, Estonia, Georgia, Buckshot Yankee Stuxnet
US Doctrine	Information warfare	Information operations	Cyber warfare

Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

Cyber warfare and Cyber terrorism

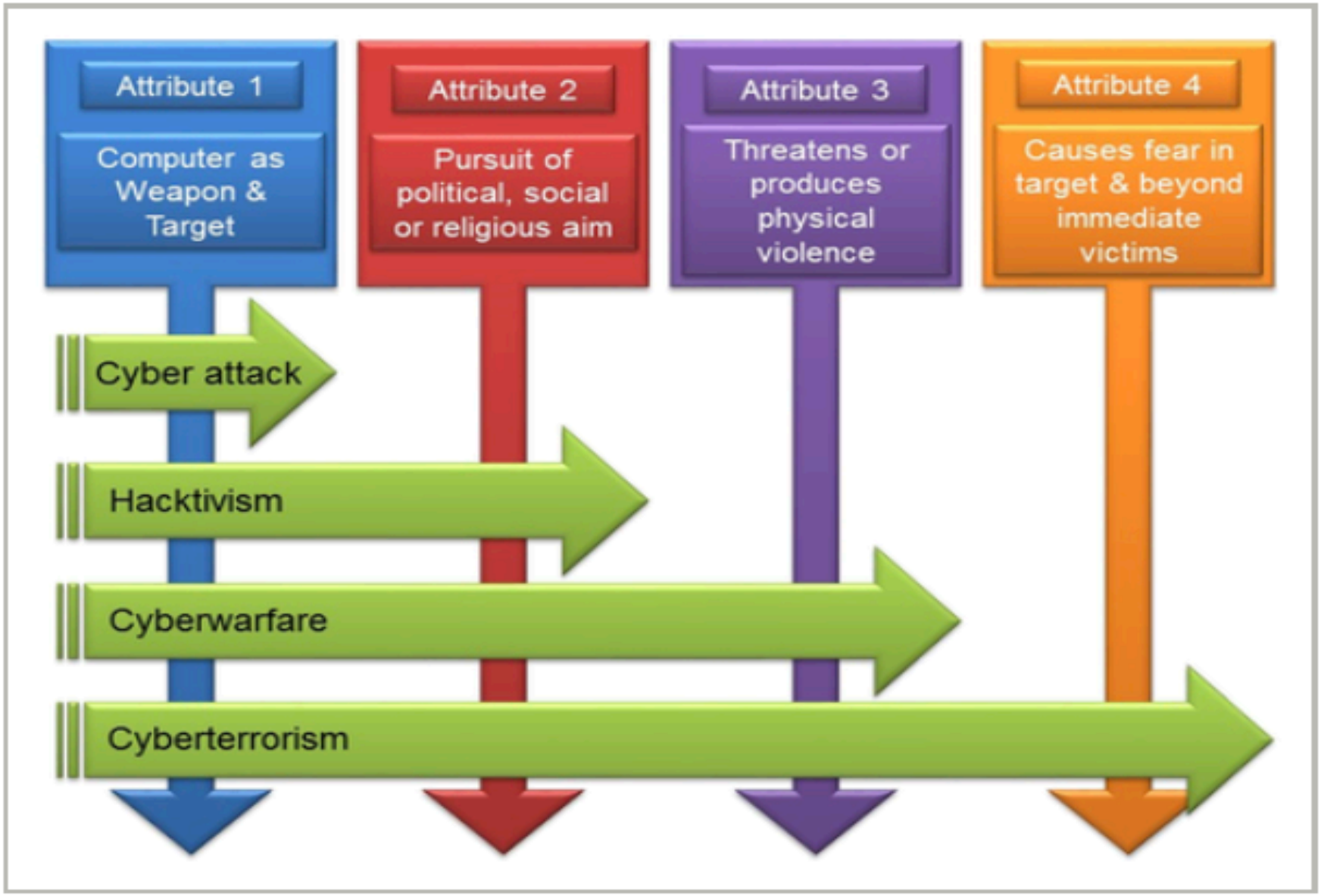
- **Cyber warfare** involves the actions by hostile foreign and domestic actors to attack and attempt to damage computers or information networks through computer viruses, social media, or voter suppression in order to disrupt and delegitimize the political system of an other country.

- **Cyberterrorism** is something done by a person or a group of hackers to inflict fear upon the victims (i.e., stealing credit cards to influence actions of a major financial corporation) or demand ransom, or steal personal identity of individuals, etc.

- Worldwide spending on **cybersecurity** will reach at least $137 billion by the end of 2022.

Four Types of Attack

- **Malware**
  - Software specially designed to disrupt, damage, or gain unauthorized access to a computer and network system (local, regional, and federal governments PLUS private sector).
- **Ransomware**
  - Is a type a malicious software designed to block access to a computer system until money is paid (i.e., Tillamook County in Oregon, the cities of Atlanta, Baltimore, Dallas, Denver, Sacramento, San Diego, and San Francisco have recently been attacked. Other cities, as well as states and localities, are similarly vulnerable.
- **Social Engineering**
  - 1. the use of centralized planning in an attempt to manage social change and regulate the future development and behavior of a society. "the country's unique blend of open economics, authoritarian politics, and social engineering”
  - 2. (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. "people with an online account should watch for phishing attacks and other forms of social engineering"
- **Phishing**
  - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers (phishing, vishing [phone calls], fake websites)



Nicholas Ayres , Leandros A. Maglaras, "Cyberterrorism targeting the general public through social Media," 11 July 2016 | https://doi.org/10.1002/sec.1568.

Hacker Threat Capabilities

Mathematical model of hacker behavior

$$M = f\,[\,P\,(v) - (c_1 + c_2)\,]$$

where:

M = Hacker motivation

P = the probability of not failing to intrude

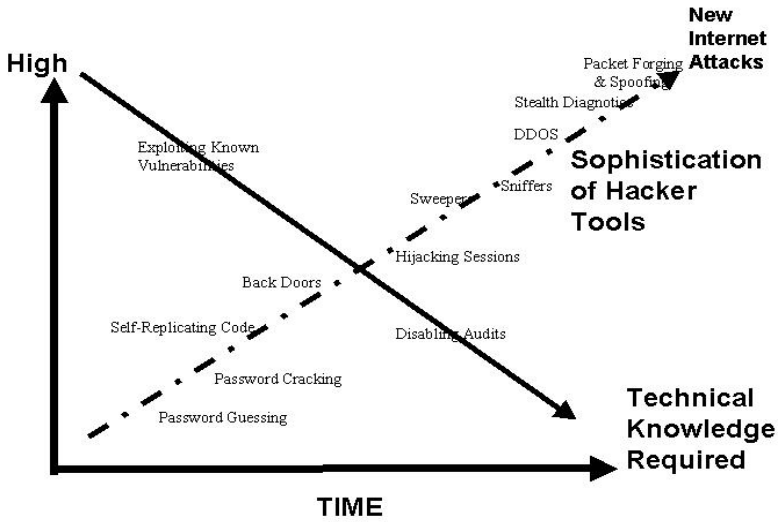
v = the value of success to the hacker

c_1 = the cost to the hacker

c_2 = the consequences to the hacker

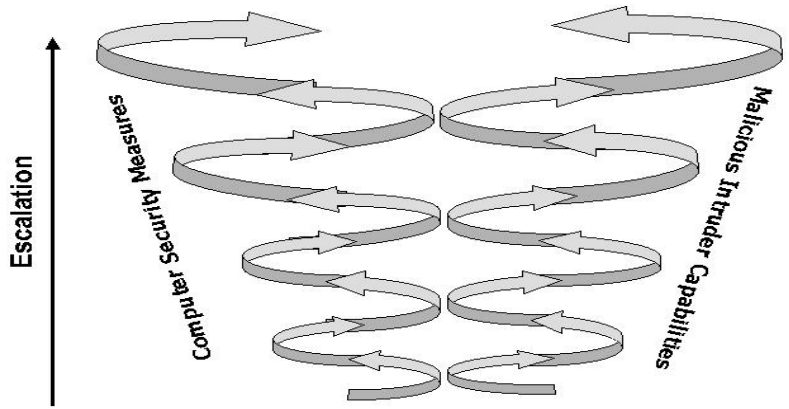
Source: H.R. Varian, School of Information Management at UC Berkeley.

+

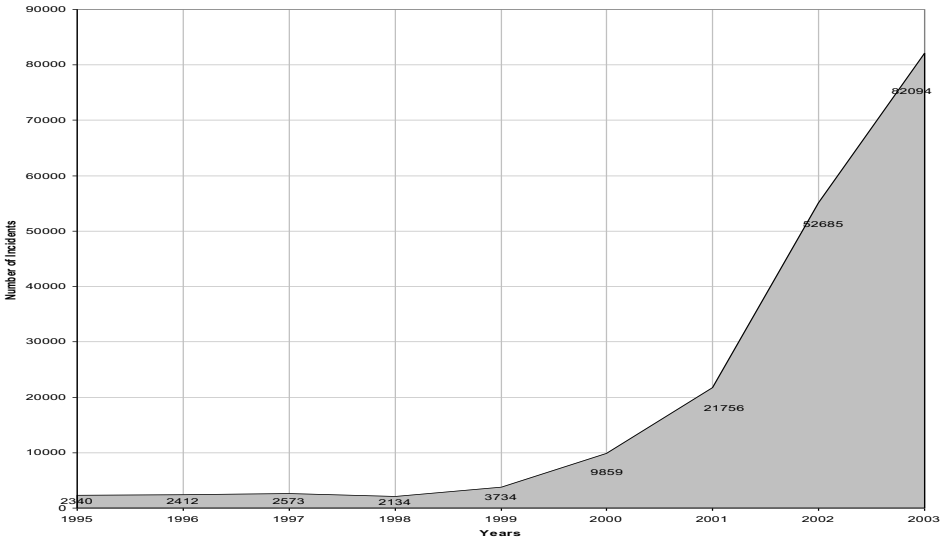


Source: TriGeo Network Security Presentation 9/23/02[2]

=

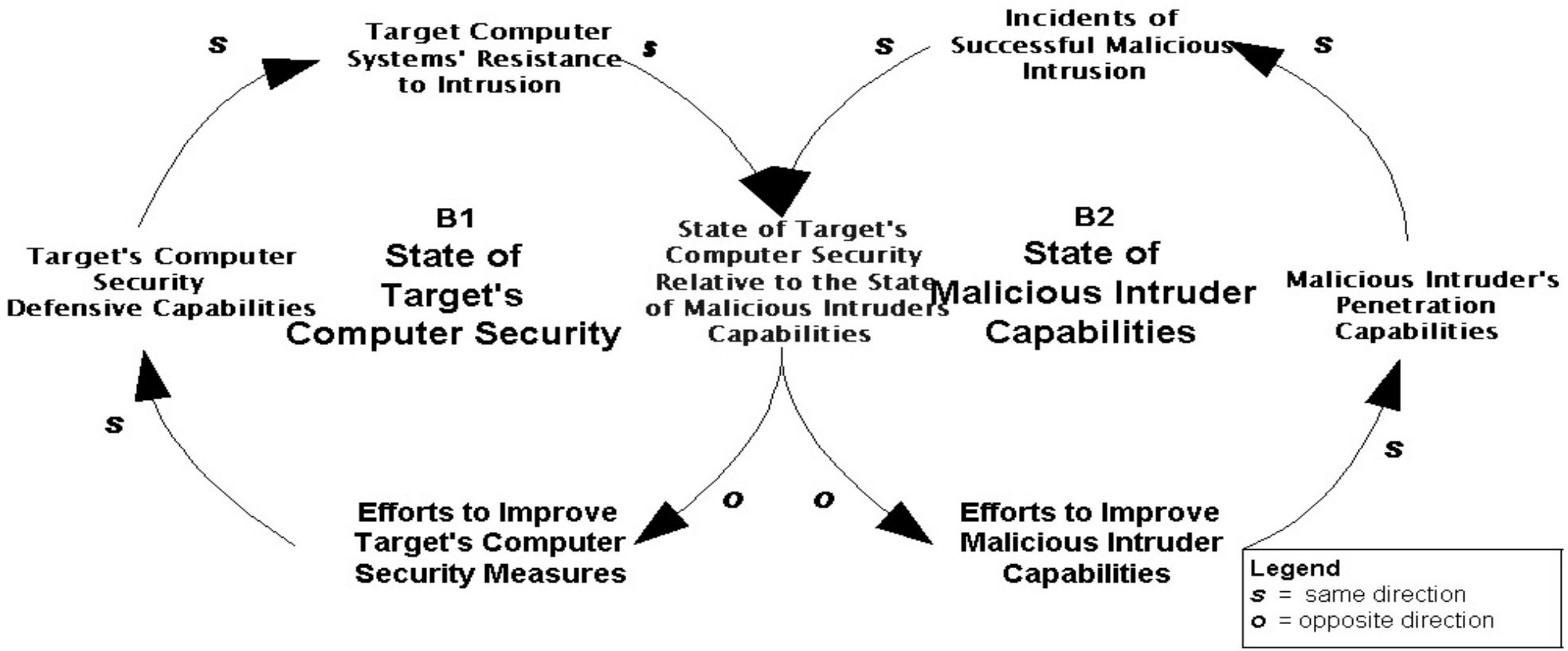


and



Proceedings of the 2006 Symposium 39th Hawaii International Conference on System Sciences
The Hyett Regency, Kauai, HI January 2006

Hackers' Arms Race Escalation Cycle



Inspired by Senge, 1990

5G expands cyber risks in 5 ways

- 1. The network has moved away from centralized, hardware-based switching to distributed, software-defined digital routing. This prevents the potential for chokepoint inspection and control.

- 2. 5G further complicates its cyber vulnerability by virtualizing in software higher level network functions formerly performed by physical appliances

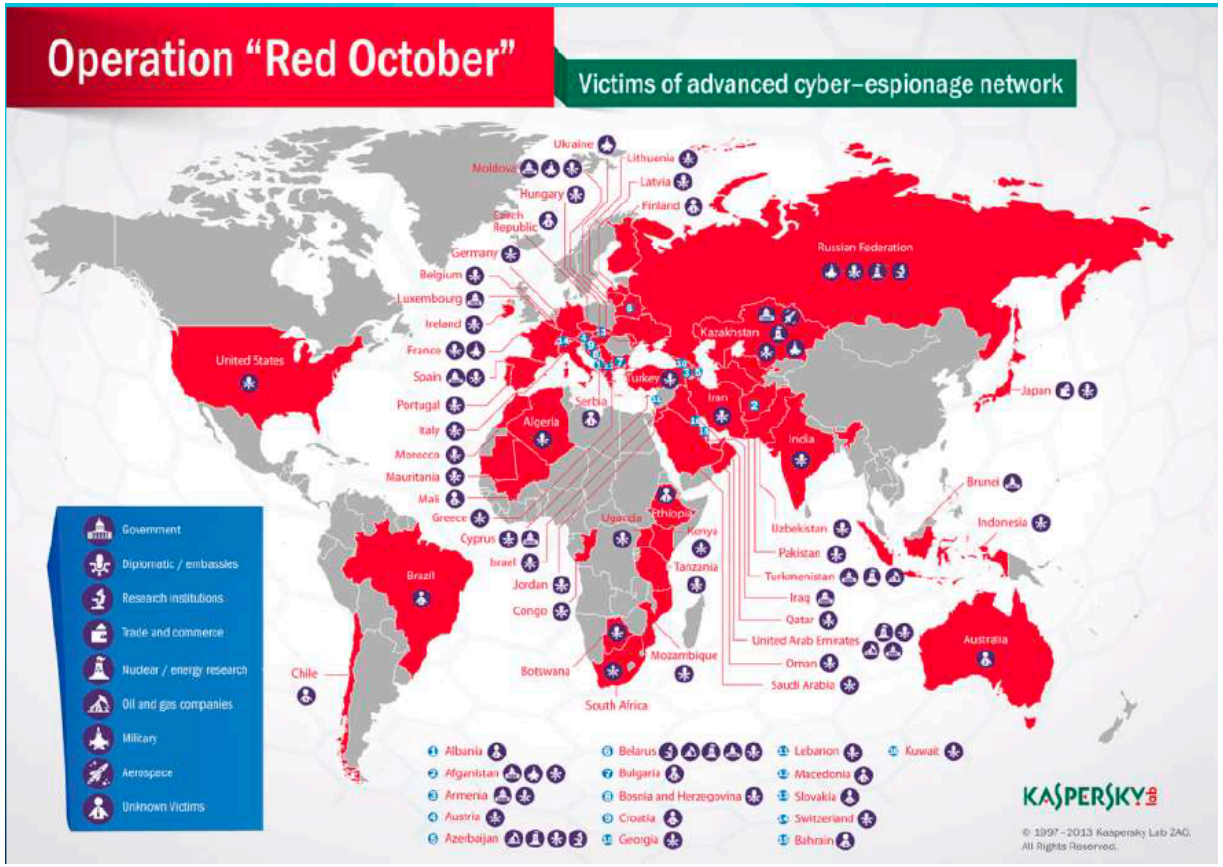
- 3. Even if it were possible to lock down the software vulnerabilities within the network, the network is also being managed by software—often early generation artificial intelligence—that itself can be vulnerable.
  - An attacker that gains control of the software managing the networks can also control the network.
- 4. The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack.

- 5. Vulnerability created by attaching billions of hackable smart devices (actually, little computers) to the network colloquially referred to as IoT.
  - In July 2019 for instance, Microsoft reported that Russian hackers had penetrated run-of-the-mill IoT devices to gain access to networks. From there, hackers discovered further insecure IoT devices into which they could plant exploitation software.

- (source: Tom Wheeler and David Simpson , “Why 5G requires new approaches to cybersecurity Racing to protect the most important network of the 21st century” Brookings, Tuesday, September 3, 2019.)

Red October (Eugene Kaspersky, co-founder of Kaspersky)

- WHEN? First discovered in October 2012 (hence the name), however the malware had been operating undetected since at least 2007.
- In October 2012, Kaspersky Lab's Global Research & Analysis Team initiated a new threat research after a series of attacks against computer networks of various international diplomatic service agencies. A large scale cyber-espionage network was revealed and analyzed during the investigation, which we called "Red October" (after famous novel "The Hunt For The Red October").



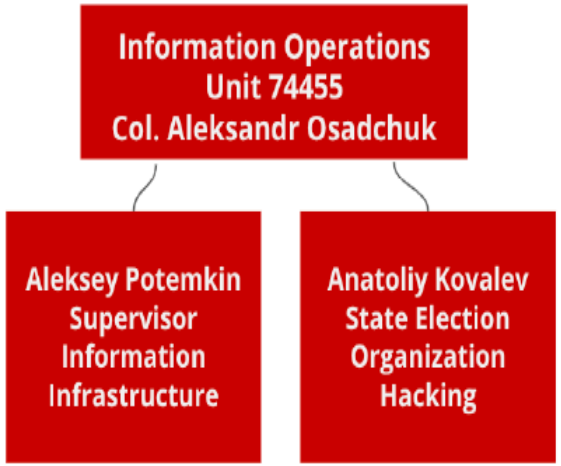
Vladimir Putin's Russia was perhaps first among major powers to deploy techniques of full-spectrum, state-sponsored disinformation for the digital age—the intentional spread of inaccurate information designed to influence societies.

1. Disruption
2. Distortion
3. Deterioration
4. Create mistrust of governments

DISMANTLE DEMOCRACIES FROM WITHIN

SECOND: frontal attacks (Estonia, NATO, Georgia, Crimea, Ukraine)

GRU/GU Units and Staff Involved in 2016 Election Interference



Russia’s cyberwar doctrine

- Russian officials are convinced that Moscow is locked in an ongoing, existential struggle with internal and external forces that are seeking to challenge its security in the information realm.
- The internet, and the free flow of information it engenders, is viewed as both a threat and an opportunity in this regard.
- Russian military theorists generally do not use the terms cyber or cyberwarfare.
- Instead, they conceptualize cyber operations within the broader framework of information warfare, a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations.
- SUMMARY: Russia’s approach is very flexible and adaptable.

Russia’s Information Warfare Doctrine

- The use of the term information warfare in American public discourse to describe Russia’s interference in the internal political affairs of other countries is problematic.

- This is in part due to the operationalization of information warfare in the United States, which is bound by the confines of legal and cultural barriers.

- Russia not only faces fewer legal and cultural barriers to influence at the operational and strategic level during both war and peace, but it also has philosophically different approaches and goals while operating in the information environment.

A Holistic Doctrine

- The Russian approach is holistic. It aims to not only affect the target state and its armed forces but also to achieve desired effects in the mind of target populations' perceptions and decision-making processes that favor Russia's interests and goals.

- This is a two-pronged approach that seeks to affect both the physical and the cognitive dimensions of the information environment.

  - At the physical level, what the Russians call the digital-technological level, they seek to disrupt and compromise the physical dimension of the information environment by penetrating, manipulating, and destroying information networks and command and control systems.

  - At the cognitive level, the Russians have already demonstrated the ability to integrate actions in the physical dimension of operations in the information environment with actions intended to affect perceptions and decision-making processes; in other words, they are achieving effects in the cognitive dimension.

The Russian view

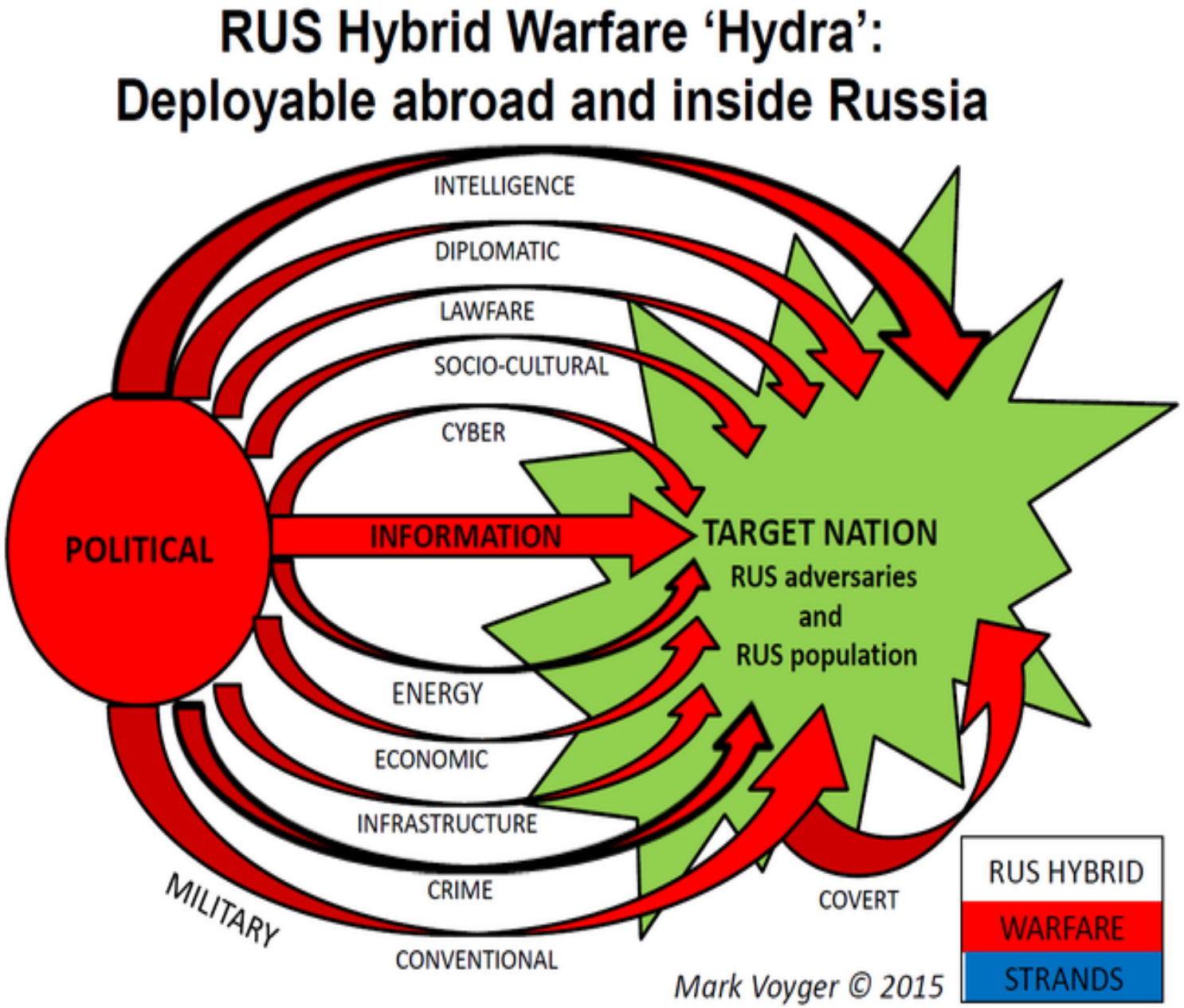
- Aleksander Dvornikov, commander of Russia's Southern Military District, points out:

> "Now states achieve their geopolitical goals through the application of complex non-military measures, which often are more effective than the military ones. The main goal of these measures is not the physical destruction of the enemy but the complete submission of his will."
>
> Aleksandr Dvornikov, "Штабы для новых войн," Военно-промышленный курьер, 23 July 2018. Russian publication *Military-Industrial Courier*

- He goes on to argue that without information operations, Russia would not have succeeded in many operations in Syria.

A Holistic Paradigm

Mark Voyger, former special advisor to retired Lieutenant-General Ben Hodges, former Commanding General of US Army Europe. (https://news.postimees.ee/4505726/mark-voyger-russian-hybrid-warfare-can-still-bring-surprises-in-the-future)



Disinformation Attacks on Democracies

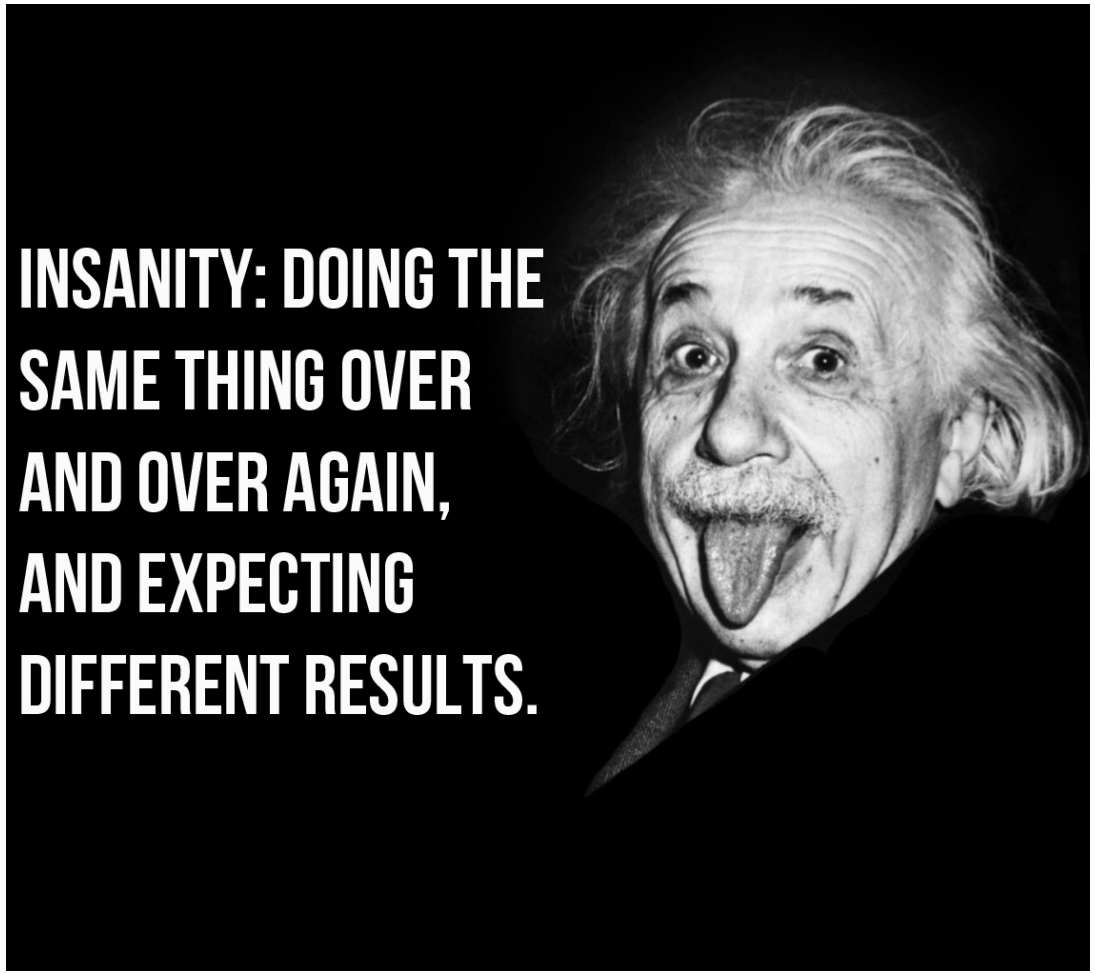
- Disinformation and democracies (Brazil, Chile, Columbia, Mexico, EU, UK, USA)
- Governments, tech and social media companies, International Organizations
- US Cybercommand
- The 2019 National Defense Authorization Act (NDAA) added significant (albeit second-order) provisions defining the importance of countering disinformation for US national security
- Major threat is Russia. Other state actors such as China, Iran, and North Korea and nonstate actors with a higher tolerance for risk, will adapt the disinformation toolkit to undermine democracies or are already doing so.

PROBLEM #1: A Severe Shortage of Cybersecurity Professionals

- The cybercrime epidemic has escalated rapidly in recent years, while companies and governments have struggled to hire enough qualified professionals to safeguard against the growing threat.

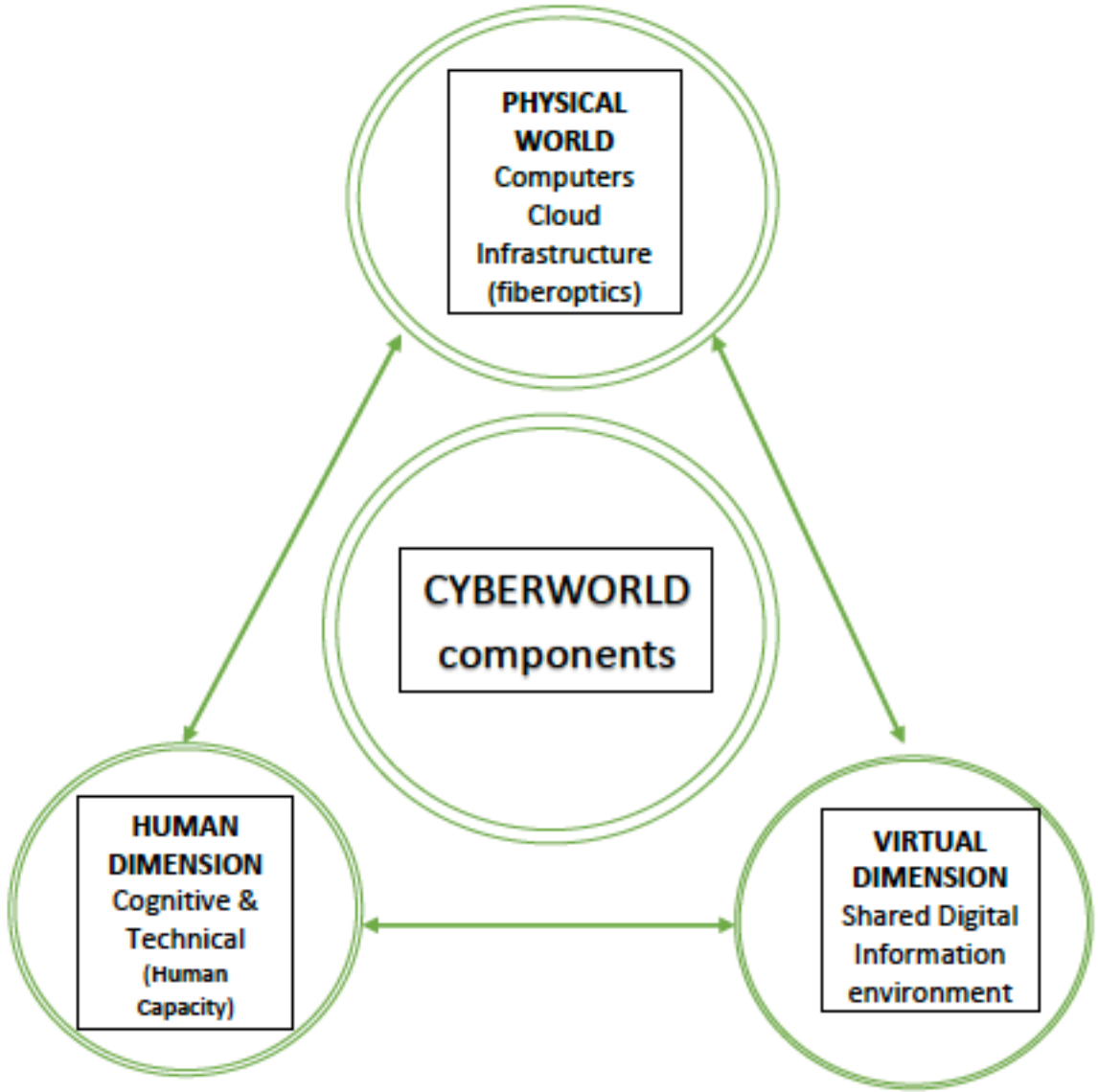
- This trend is expected to continue into 2020 and beyond, with some estimates indicating that there are some 1 million unfilled positions worldwide (potentially rising to 3.5 million by 2021).

Problem #2: Definition of Insanity



Changing US Gov. Cybersecurity Preparedness Model

- Revise the Education and workforce training
- Address decline in Higher Ed – Gov – Private Sector Partnership (similar to the Manhattan Project and beyond)
- Address what-if scenarios for 5, 10, years in the future.


PHYSICAL WORLD
Computers
Cloud
Infrastructure
(fiberoptics)
CYBERWORLD components
HUMAN DIMENSION
Cognitive & Technical
(Human Capacity)
VIRTUAL DIMENSION
Shared Digital Information environment

U.S. CYBERWAR DEFENSES

- Department of Defense (specifically the U.S. Cyber Command) – defends military assets against cyber threats and maintains offensive capabilities
- Department of Homeland Security – defends civil and commercial assets against cyber threats, including critical infrastructure systems
  - United States Computer Emergency Response Teams (US-CERT) – defends the United States' Internet infrastructure against cyber threats along with coordinating responses to cyber attacks

In the years to come, cyber warfare will likely become as common as traditional warfare, leading many to believe a new branch of military dedicated to cyber warfare will emerge.

Vulnerability identification

- **Networks**
  - Poor physical security, management, port security, Firewall, anomaly detection
- **Configuration**
  - Poor account management, passwords, patch management, ineffective detection programs
- **Platforms**
  - Lack of system update, insecure applications, untested third-party applications, patch management
- **Public Policy (Domestic and National Security)**
  - Inexperience personnel, inadequate security awareness, insufficient training for social engineering recognition, physical security, weak access control, outdated policies
  - *Workforce training above and beyond IT (Engineering and Computer Science)*

The *soft-underbelly* of the United States: Local and Regional Governments

- Cyber attack through local and regional governments, NGOs (that work with local and regional authorities, USPS, and power grids).
- The enemy can enter the national cyber network through the BACKDOOR.
- Made much easier to attack through **5G technology**.

PROBLEM #3: Future Workforce Training and R&D

- Definitional Problem – what is cybersecurity?
- Do we need an International Cyberspace Treaty (International Regime) - legal experts?
- Revise the Preparedness Model
- The Levels of Analysis Problem
- Public-Private Partnership

Cybersecurity: A new Perspective

- How would you define cybersecurity in order to address both security and defense?

- **C *(f)* = P + I + Hc + M + T**

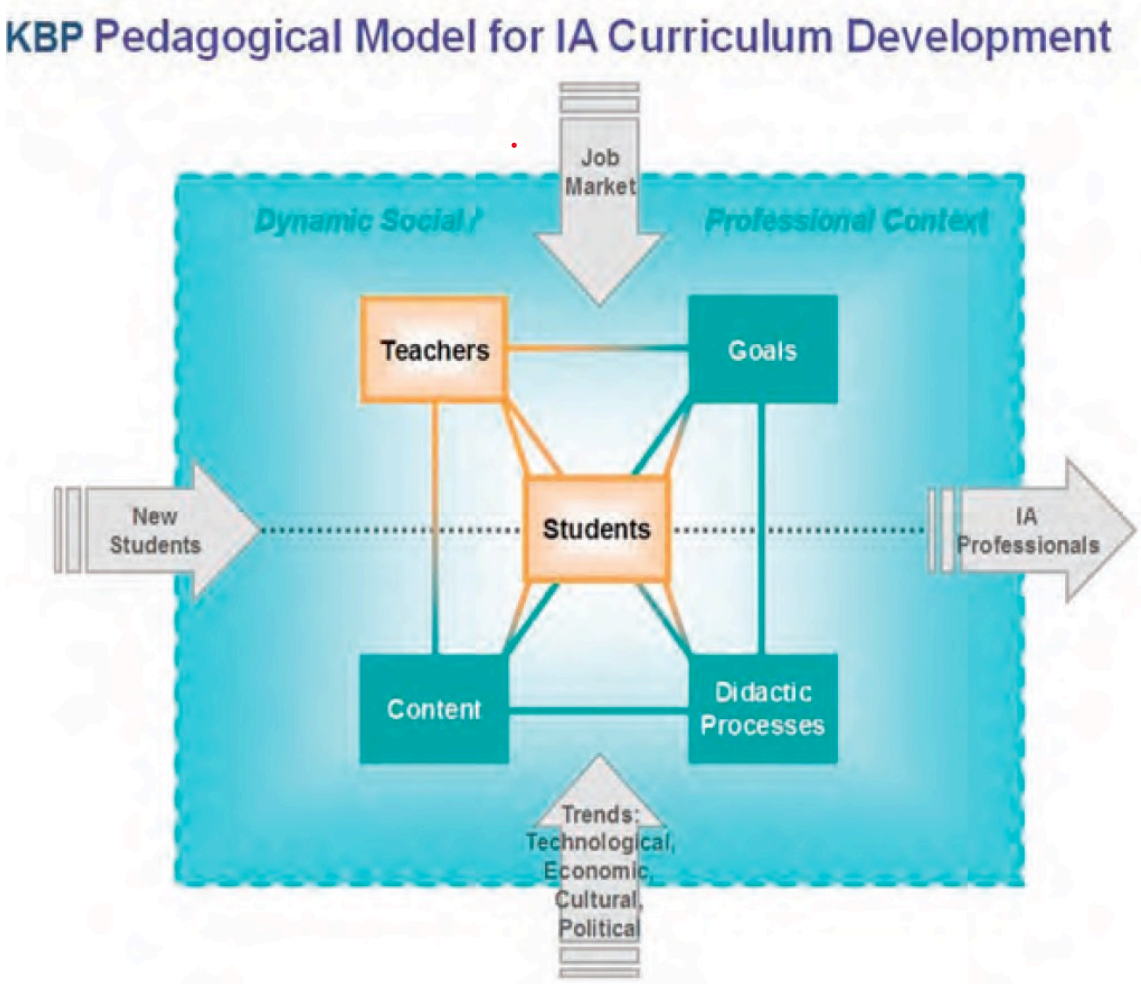
- Where;
- P= Policy,
- I = Policy implementation,
- Hc = Human capacity, *cognitive DM capacity leads to perceptions and misperceptions*
- M = Management, and,
- T = Technology

- *This is where the challenge lies: between public policy, technology and collaborative governance.*

Education Remedy

- ~~Russian Remedy~~
  - Goal: Cheslavik (Numbers Person)

- Proposed Response
  CIAC UW + PSU
- A Bridge Between
  Technology/CS and Public Policy
- Goal: Tech + Cultural, socio-economic-political and Language Awareness (Holistic person)



SYSTEMS THINKING CONTEXT

Attribute	Agricultural Age	Industrial Age	Information Age
Wealth	Land	Capital	Knowledge
Advancement	Conquest	Invention	Paradigm Shifts
Time	Sun/Seasons	Factory Whistle	Time Zones
Workplace	Farm	Capital equipment	Networks
Organization Structure	Family	Corporation	Collaborations
Tools	Plow	Machines	Computers
Problem-solving	Self	Delegation	Integration
Knowledge	Generalized	Specialized	Interdisciplinary
Learning	Self-taught	Classroom	Online

Inspired by Covey 1989

The Levels of Analysis Challenge: Horizontal and Vertical Integration

- Local to Systemic levels of analysis & training of new workforce
- Public-Private partnership (lateral partnership of key stakeholders).
  - Educational institutions, private companies, government, and citizens.
- Multi-tools training including languages, cultures, history, law, politics, and methodologies.

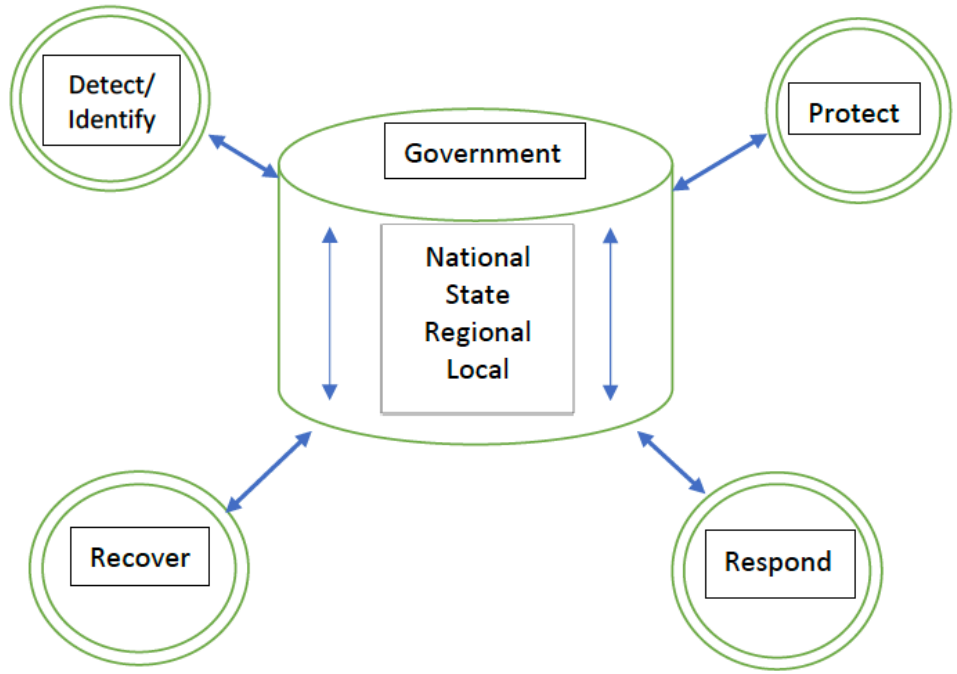
International System

Nation States

Federal/Regional Governments

Local Government (The Soft Underbelly)

{PRIVATE SECTOR + NGOs + PUBLIC SECTOR}



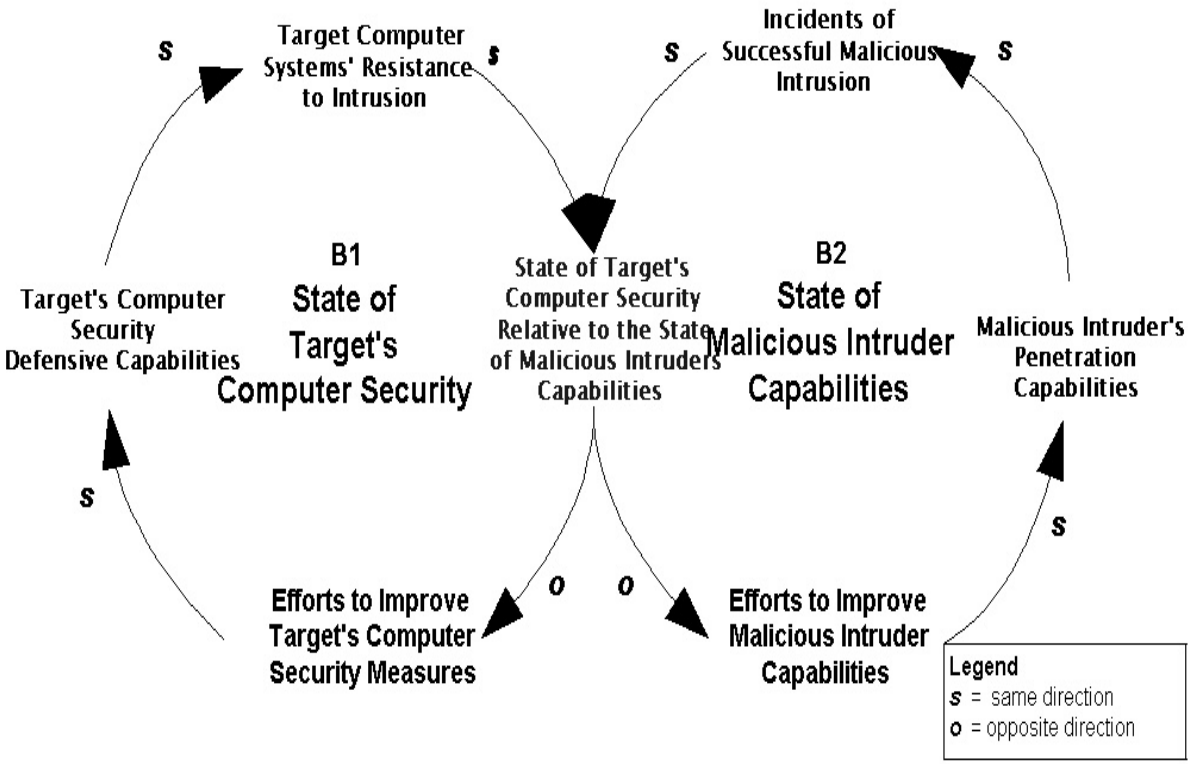
Where PSU's CAE-R and future CAE-CDE Fit?

- A Comprehensive and Collaborative Research and Education between Colleges: An interdisciplinary Approach to Cybersecurity
    - The Hatfield School of Government – public policy, legal challenges, local/regional/state governance, national security.
    - The Toulan School – Urban Planning & Studies, Population Studies
    - College of Engineering - cloud research, computer science, engineering and technology management, smart cities.
    - School of Business Administration – Block chain and privacy, Language, culture, and history.
    - College of Liberal Arts and Sciences – culture, history, language.
    - PSU-UW
    - PNNL-UW-PSU
- Horizontal and Vertical integration of analysis (local to global AND public-private) – *A Systemic Conceptualization of the Problem.*

Disrupting the Hackers' Arms Race System: Inserting the Human

Technology TOOLS

Survivability Strategy	Tools
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react or adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • Replication • Backup systems • Fault tolerant designs

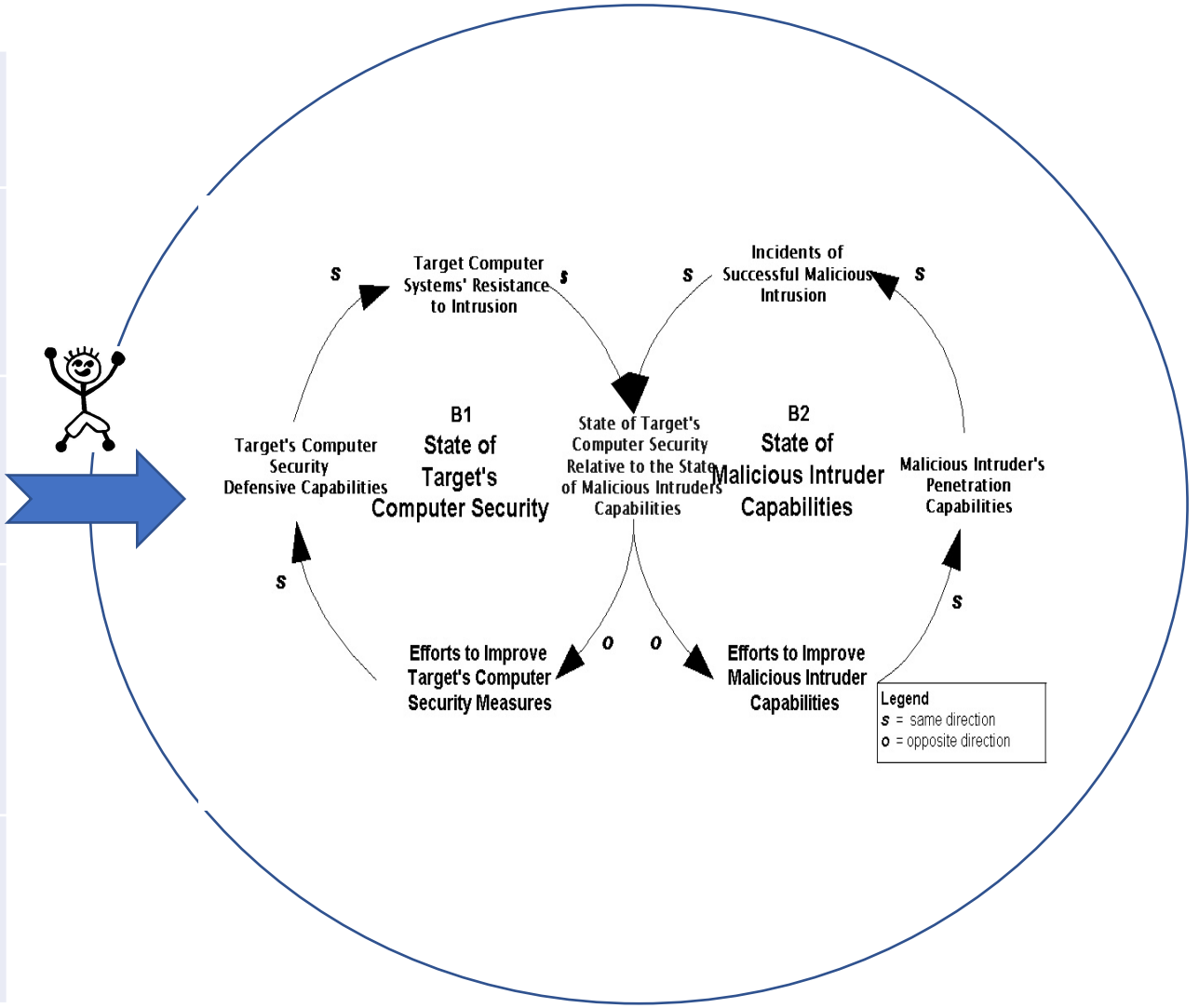


Adding the Human Factor: Cognitive Neuroscience Meets The Cyberworld

"Cybersecurity is intimately bound up with non-cyber!" (Matt Bishop, UC Davis)

Adding the Human

Survivability Strategy	Tools
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react or adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • Replication • Backup systems • Fault tolerant designs
1)Ability to hold intruders accountable in a court of law. 2)Ability to retaliate	• Computer Forensics • Legal remedies • Active defense



Thank You for Listening any Questions?