Can we handle a Cybrid crisis without AI/ML?

@ ENISA conference: Artificial Intelligence – An opportunity for the EU cyber crisis management
3-4 June 2019, Athens

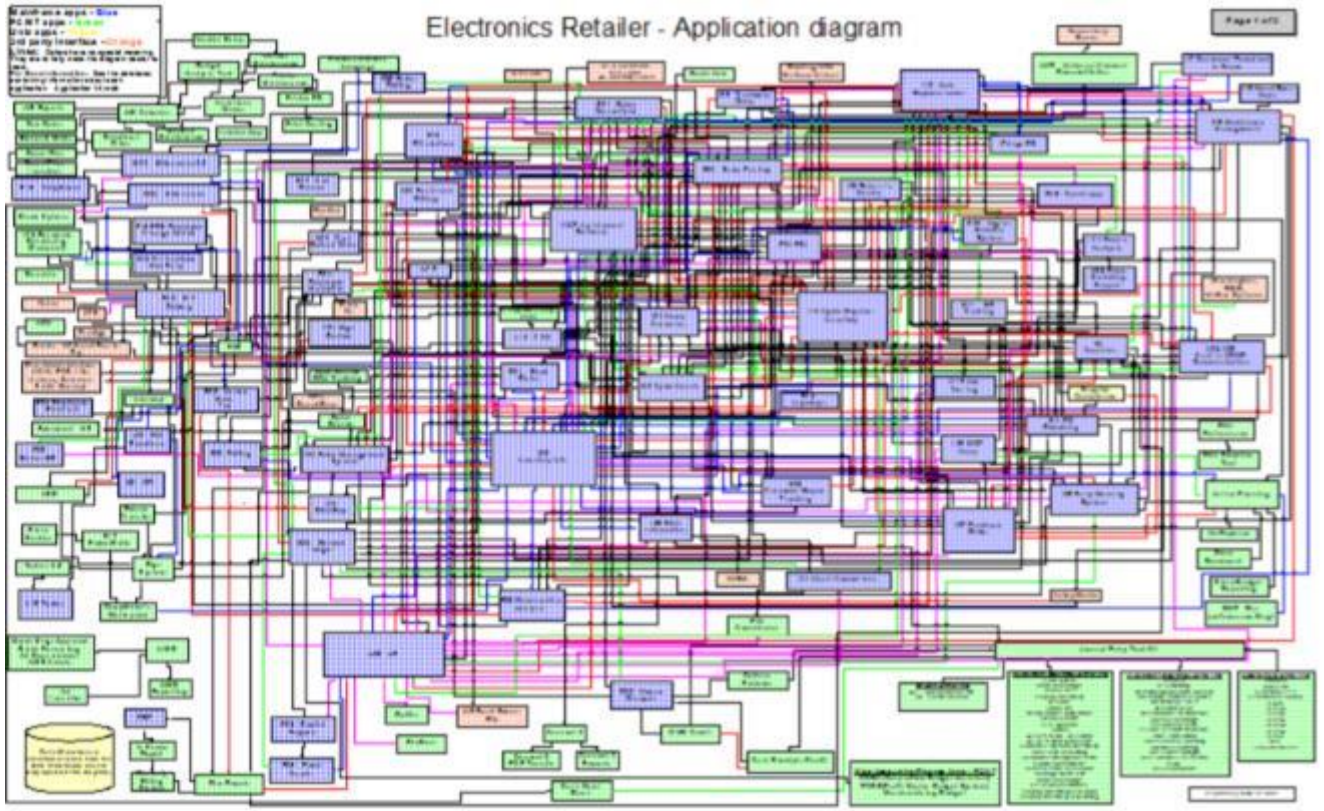
Dr. George Sharkov

Adviser Cyber Defense @ MoD - g.sharkov@mod.bg

National Cybersecurity Coordinator (2014-2017)

Director, European Software Institute CEE & Cyber Security & Resilience Lab

Digital dependency, interoperability and complexity >>> new types and levels of vulnerabilities



Application complexities

Business process complexities

and more…

Digital dependency and complexity:

If Software is eating the world,
are we safe ?

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Lif

2011

ESSAY

Why Software Is Eating The World

By MARC ANDREESSEN

August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the future growth of the American and world economies, despite the recent turmoil in the stock market.

In an interview with WSJ's Kevin Delaney,

In short, software is eating t

More than 10 years after the dot-com bubble, a dozen or s companies like Facebook an sparking controversy in Silic their rapidly growing private valuations, and even the occ

2016

ANDREESSEN HOROWITZ

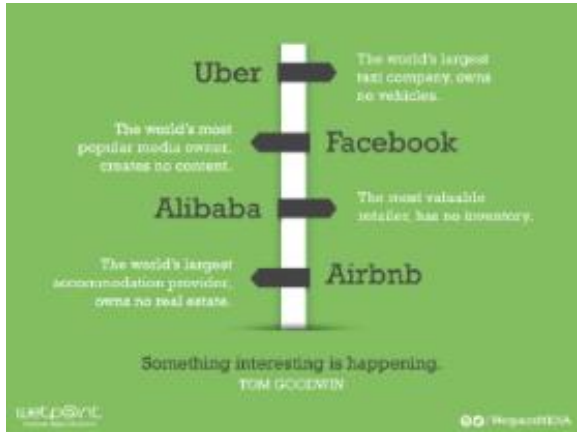
Software Is Eating the World

MACHINE & DEEP LEARNING

a16z Podcast: Software Programs the World

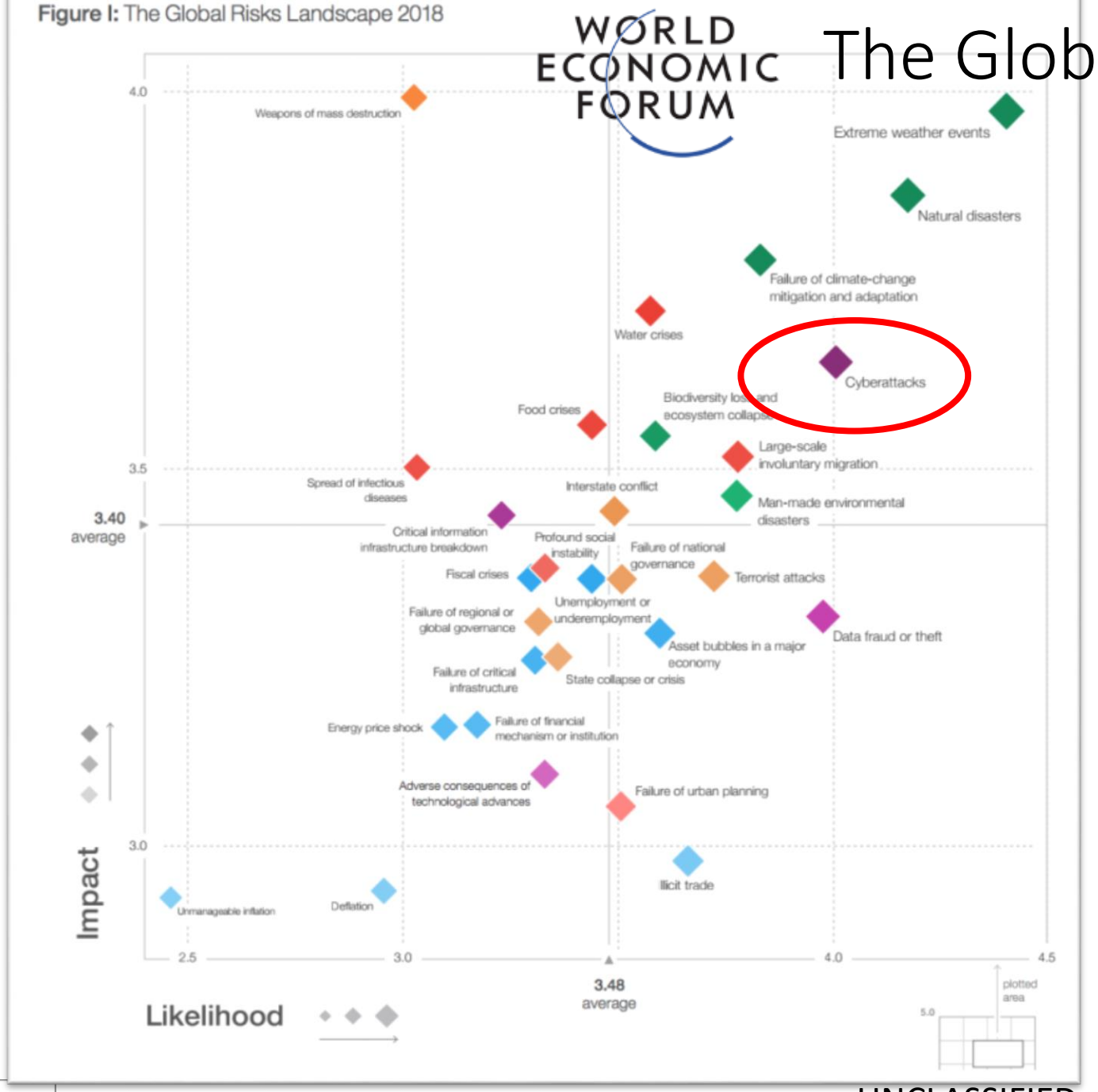
with Marc Andreessen, Ben Horowitz, Scott Kupor, and Sonal Chokshi

"All of a sudden you can program the world" — it's the continuation of the software eating the world thesis we put out over five years ago, and of the trajectory of past and current technology shifts. So what are those shifts? What tech trends and platforms do we find most interesting on the heels of raising our fifth fund? Are we just building on and extending existing platforms though, or will there be new platforms; and if so, what will they be? Well, distributed systems for one...



… distributed systems — encompassing cloud and SaaS; A.I., machine learning, deep learning; and quantum computing — to the role of hardware; future interfaces; and data, big and small.
… why simulations matter… and what do we make of our current reality if we are all really living in a simulation as Elon Musk believes?

The Global Risk Landscape - 2018



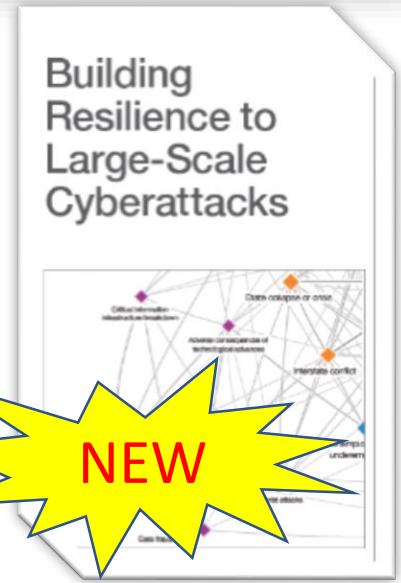
January 25, 2018, Davos

To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity

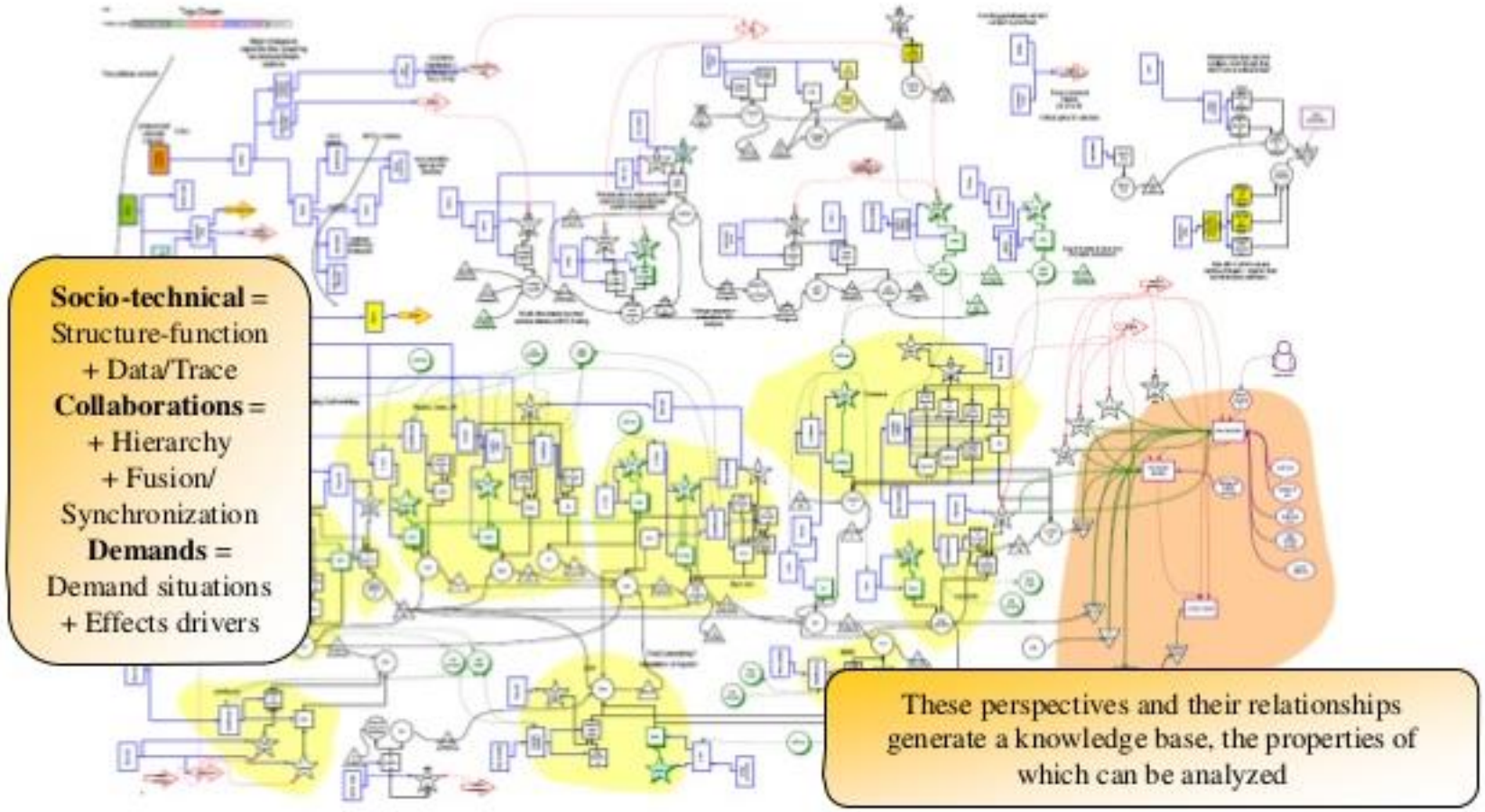
1. Building Resilience to Water Crises

2. Building Resilience to Large- Scale Involuntary Migration

3. Building Resilience to Large- Scale Cyberattacks



Understanding cyber/hybrid crisis:
Digitized Society (the “fifth domain”) = digital “ecosystem” of
1) Cyber-Physical Systems
2) Complex Systems-of-Systems with emergent behavior



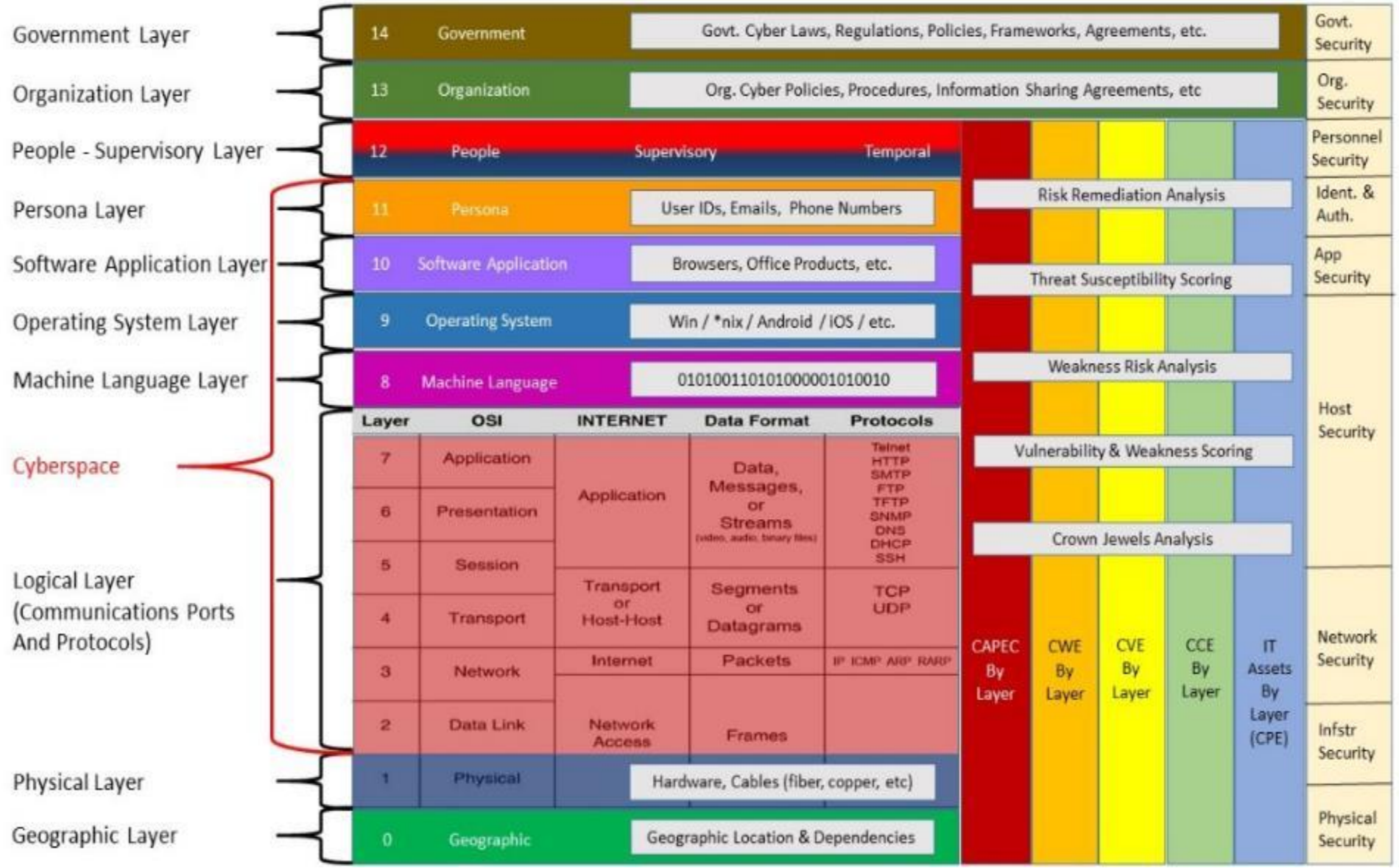
Complex Systems-of-Systems (SoS) Interoperability layers and security

- Network Transport – physical connectivity and network interoperability;
- Information Services – data/object models, semantic/ information interoperability, knowledge and awareness of actions interoperability;
- People, Processes and Applications: aligned procedures, aligned operations, harmonized strategy/doctrine, and political or business objectives.

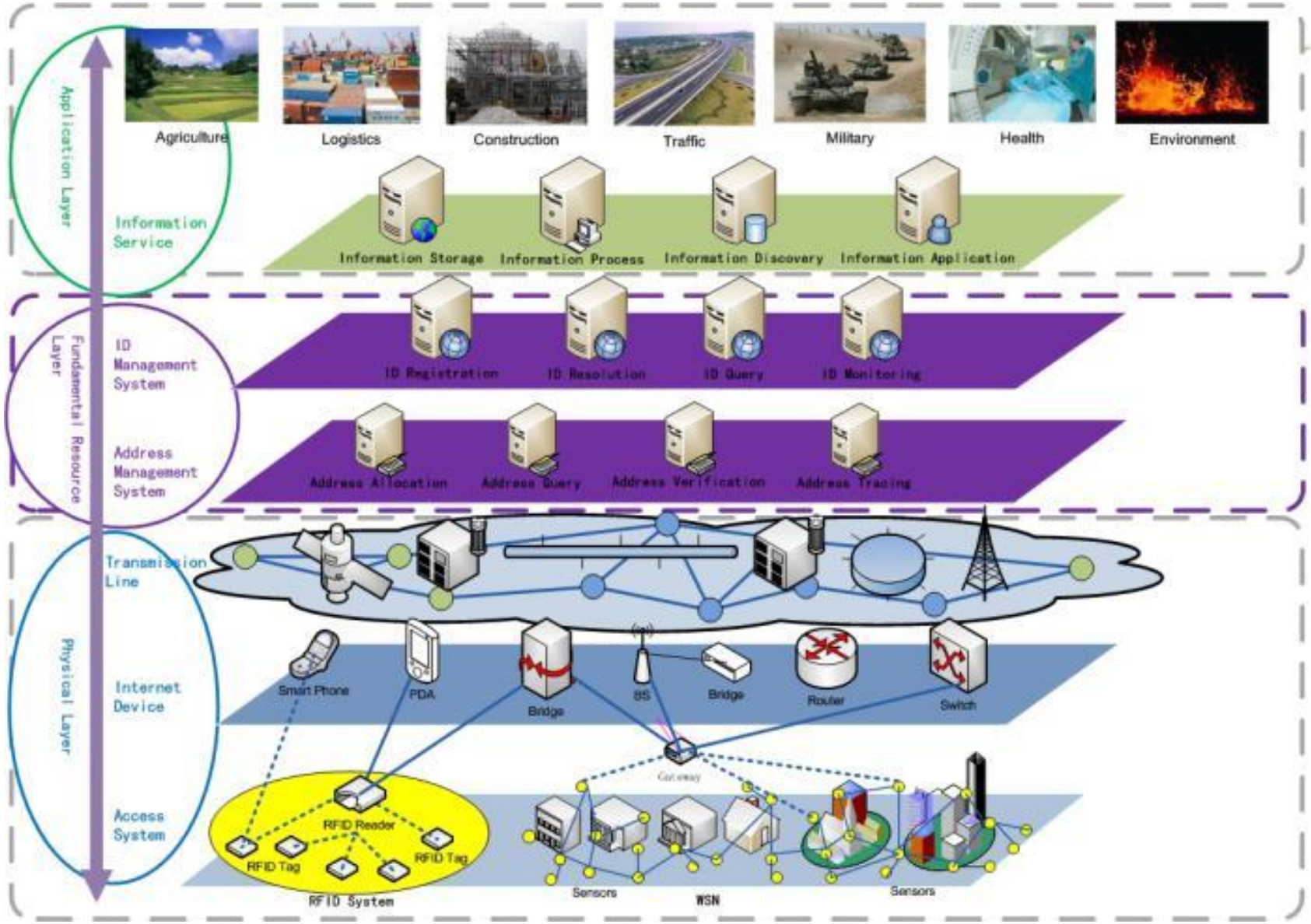
Holistic approach – understanding interdependencies:

Beyond Layer 7: the real Cyberspace and Cyber terrain

[DoD - Defense in depth; Cyber Physical Systems]



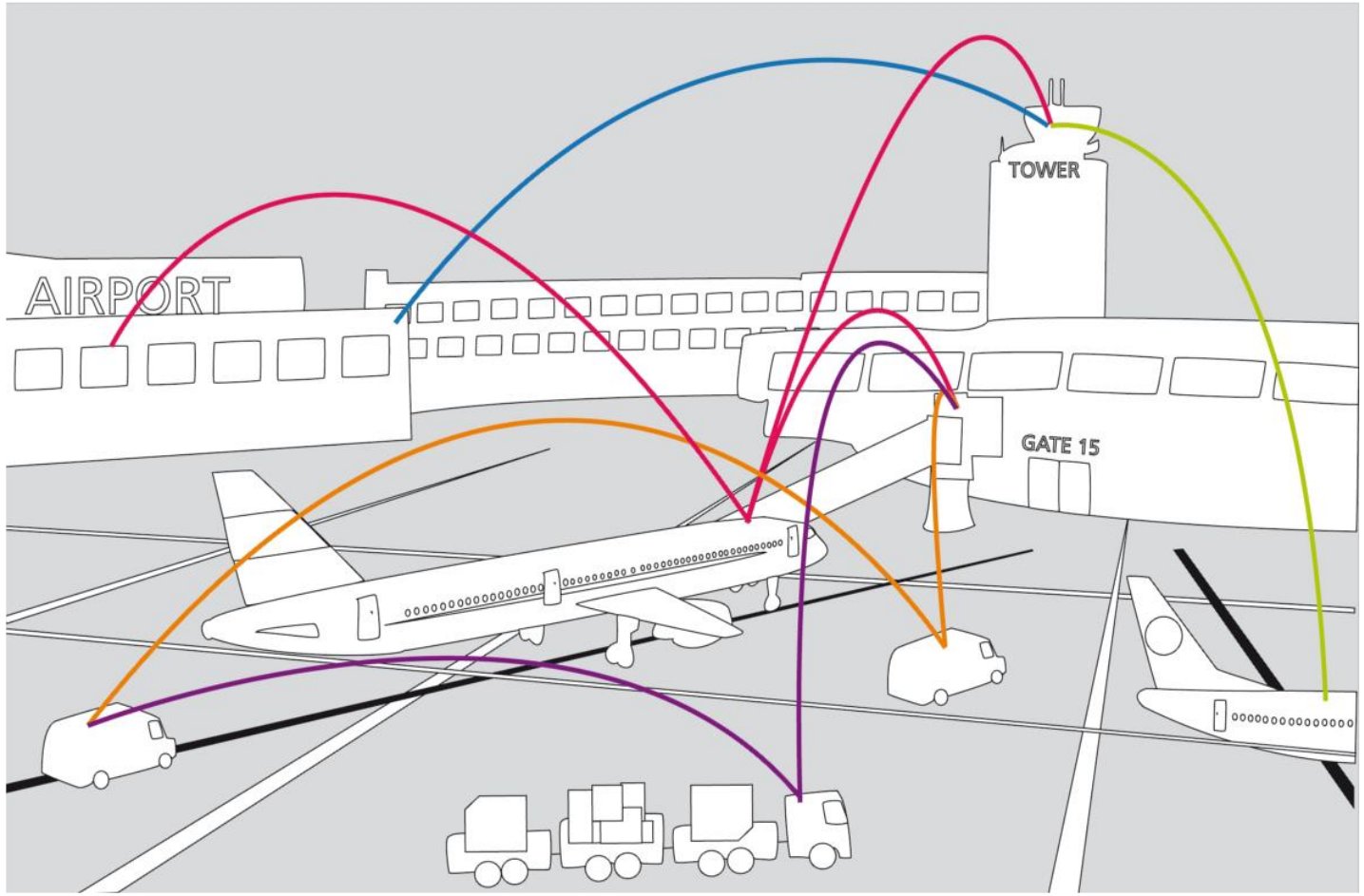
SoS and Layers of the IoT/IIoT



Understanding SoS (emergent) behavior

≠

Sum of compound systems



SoS are not just complex systems

[Maier's criteria, 1998]

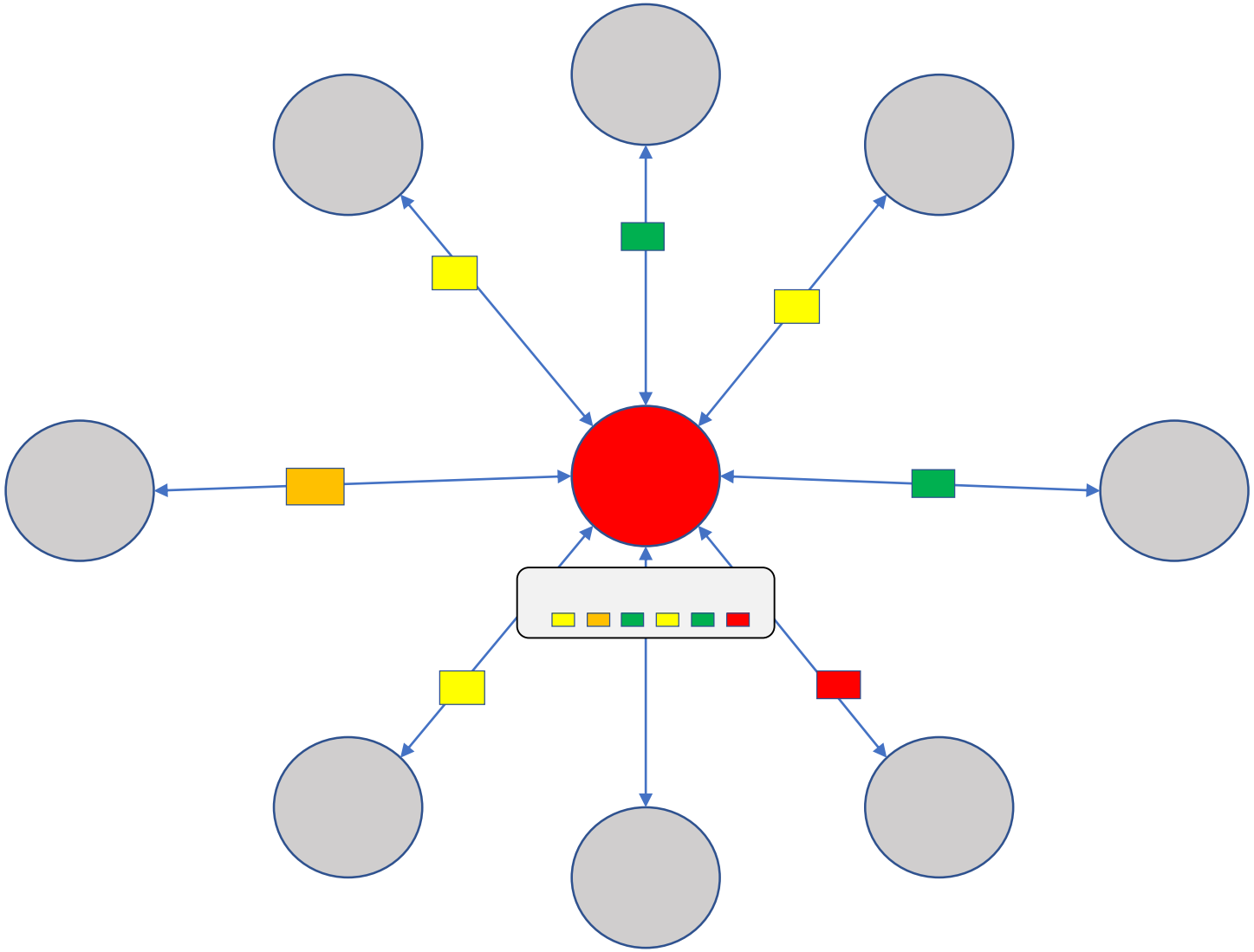
- Operational Independence of Elements
- Managerial Independence of Elements
- Evolutionary Development
- Emergent Behavior
- Geographical Distribution of Elements

[Dr. Daniel DeLaurentis, 2005]

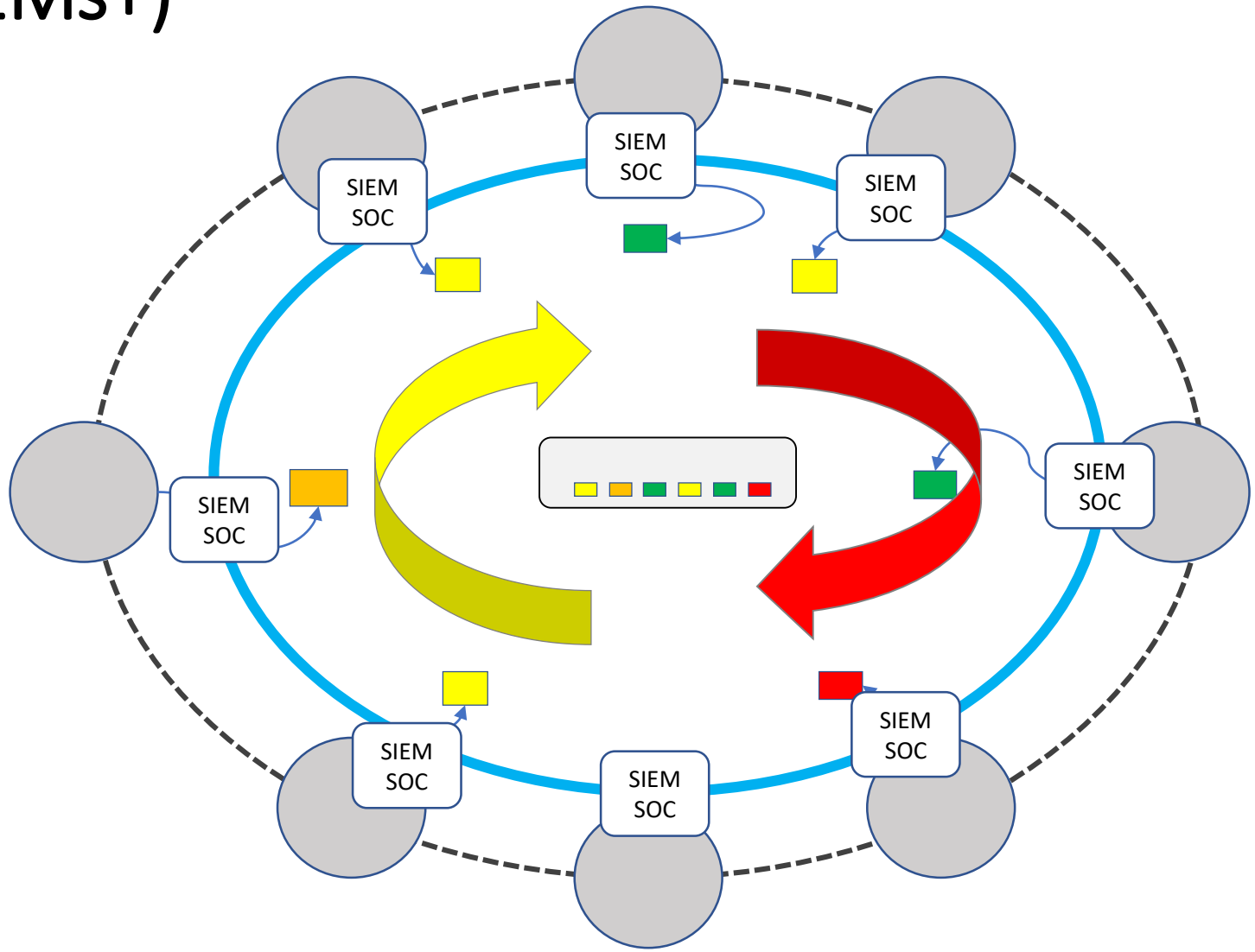
- Interdisciplinary Study
- Heterogeneity of Systems
- Networks of Systems

SoS (System-of-systems) need AI/ML for “management”

SoS: Situational Awareness view (simplified)



SoS Resilience = SIEM/SOC collaboration, AI/ML empowered (advanced SIEMs+)



Threat/Vulnerability side

- SoS (Systems-of-Systems) and emergent behavior/risks
  - From Very-large-scale systems to all interoperable systems
  - Cyber Physical Systems
  - Supply Chains as SoS
- Micro-targeting
  - Privacy
  - Mind/behavior manipulation
- “Embedded” (by design) vulnerabilities (exploitable?)
  - Zero day
  - “Eternal Blue” Syndrome
  - Complex nature
- Unknown Unknowns

Economy, state and society:
from cyber hacking to manipulation of emotions and minds

Behavioral microtargeting

The New York Review of Bo

Subscribe | Current Issue | NYR Daily | Calendar | Archive | Classifieds

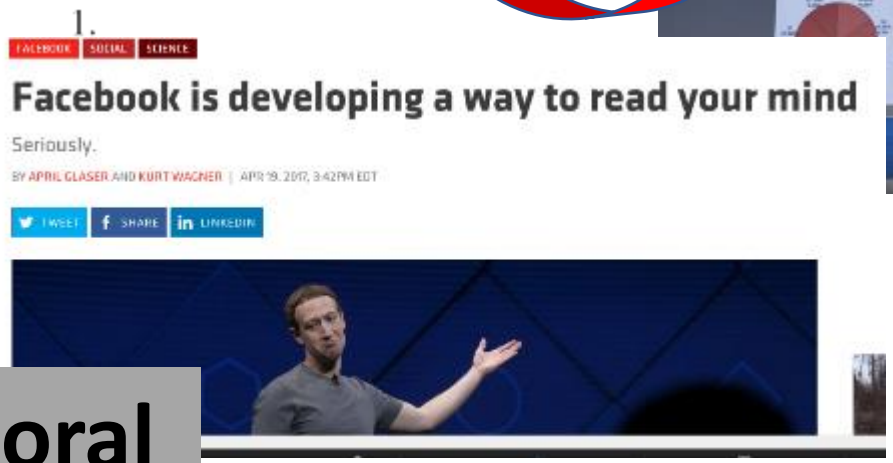
EMAIL PRINT

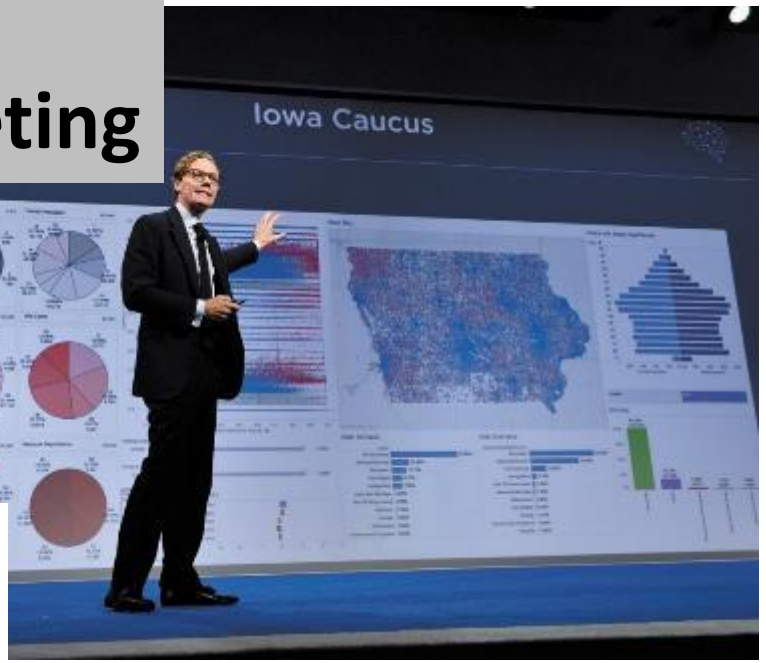
Invisible Manipulators of Your Mind

Tamsin Shaw

APRIL 20, 2017 ISSUE

The Undoing Project: A Friendship That Changed Our Minds
by Michael Lewis
Norton, 362 pp., $28.95





Concordia Summit: Alexander Nix, the CEO of Cambridge Analytica, which did data analysis and message targeting for the Trump campaign, New York City, September 2016

Behavioral economics

SoS - obvious and non-obvious relationships and linkages Forensic vulnerability analysis: the weak point is at 4th Degree of Separation

Figure 1. Identifying Centers of Gravity

Source: Joint Publication 2-0, IV-14.

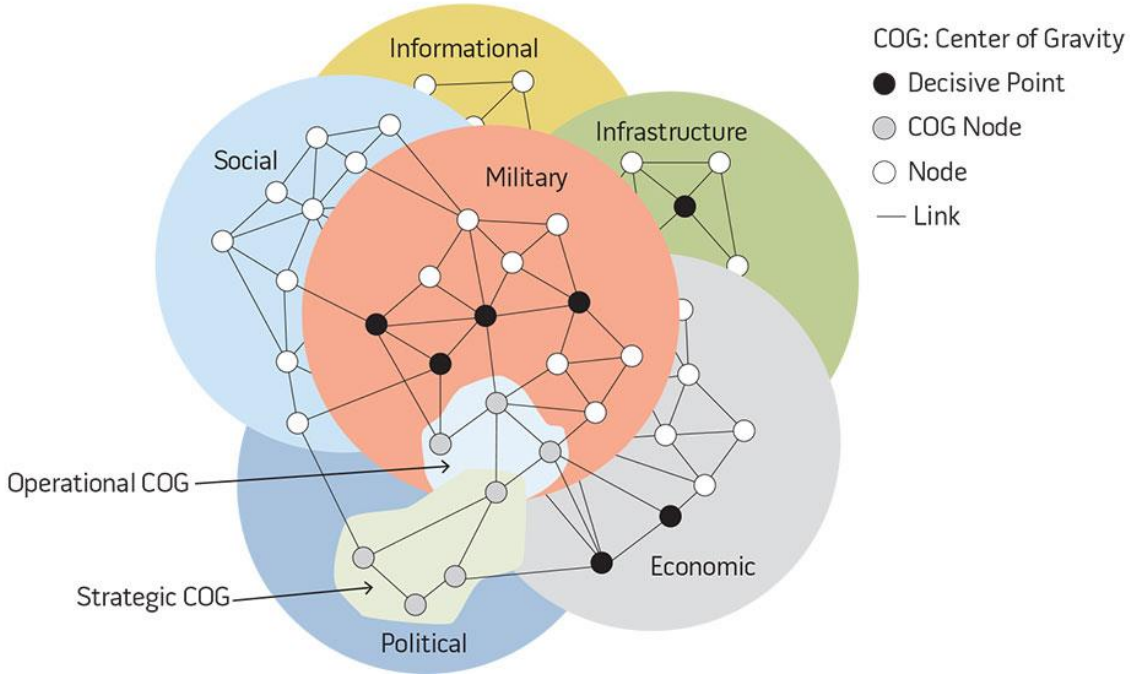
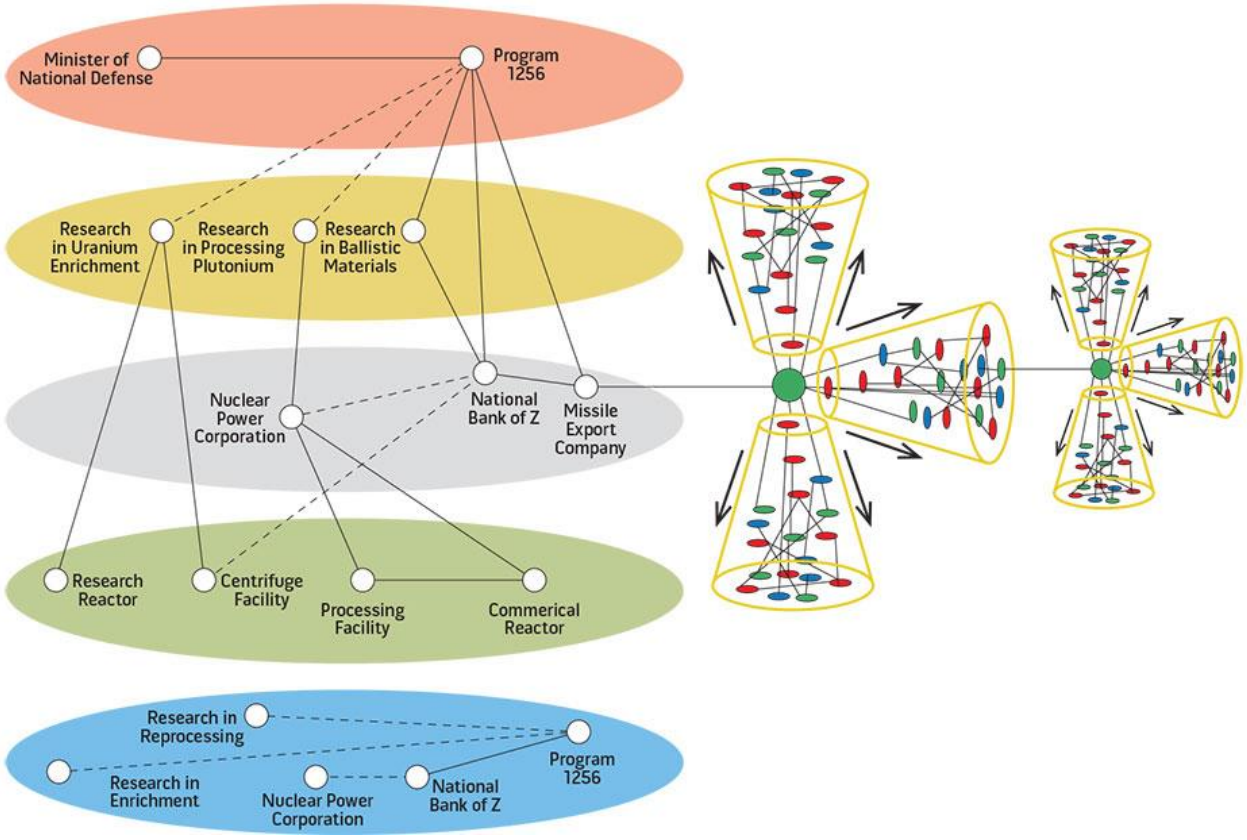
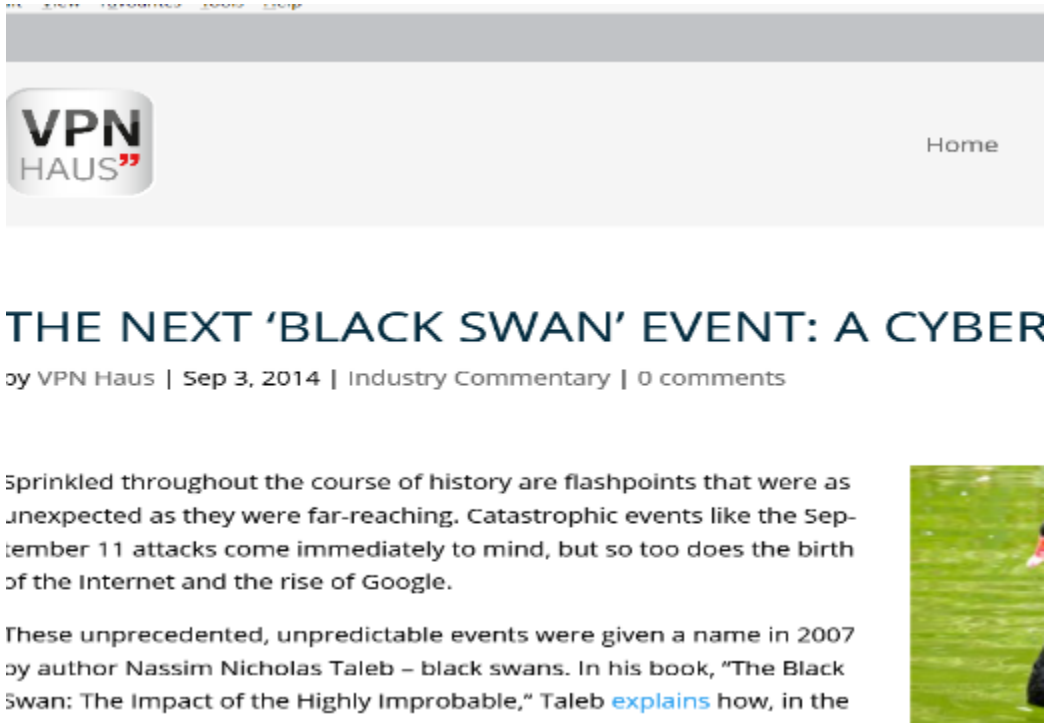


Figure 3. Interconnected and Global System of Systems



https://ndupress.ndu.edu/Media/News/Article/1130658/forensic-vulnerability-analysis-putting-the-art-into-the-art-of-war/

Unknown unknowns = ontological uncertainties



Need: **Prepare Organizations and Nations for “Unknown Unknowns”**

Protection / Defense / Resilience side

- Security & Resilience by design
  - IoT (+ Industrial Control Systems ICS/SCADA)
  - Requirements CIP, CIIP, Essential Services
- Regulations - eID (eIDAS) – in relation to GDPR, NISD, PSD2
- Standards, certifications – holistic approach (entire ecosystem), complementarity
- New generation SIEMs
- AI – more than Machine Learning
- Quantum Safe Cryptography
- Active response capability development

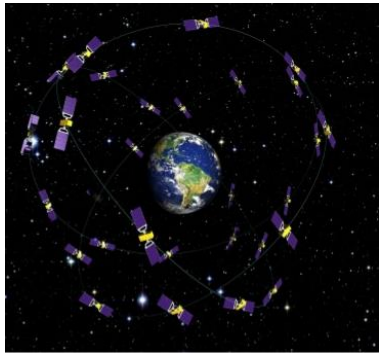
If AI/ML is already in charge, can we have situational awareness and impact assessment without?

[the Blueprint]

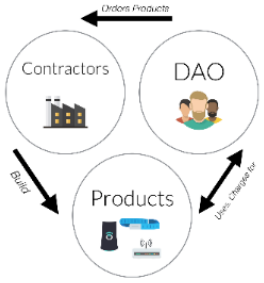
Energy: Nuclear Power Plants

Utilities: Water Plants/Electrical Grid

Military: Nuclear / autonomous Weapons



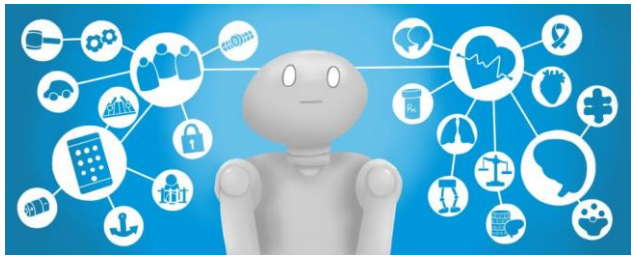
Communications: Satellites



Supplies/Logistics: Supply/Value chains

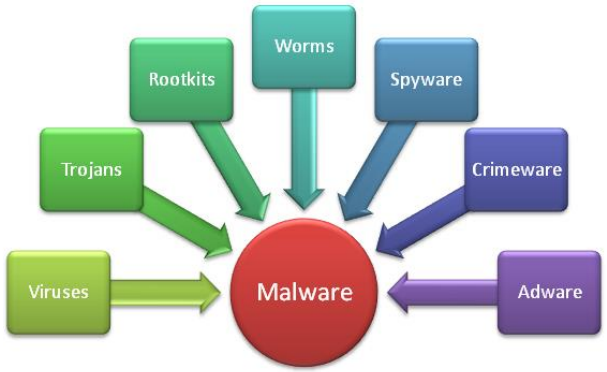
Financial/Stock Markets: >80% generated by Automated Trading Systems

Aviation: Uninterruptible Autopilot System, Training simulators



Science: R&D, Applied, Education

Super Viruses – Weaponized AI/ML



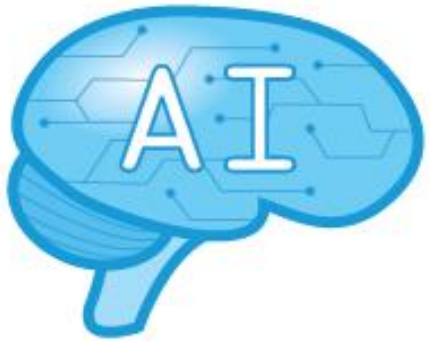


Table. Adversarial Technology Examples

Adversarial Technology	Year	Financial Impact	Users Affected	Transmit Vector
"I Love You"	2000	$15 billion	500,000	Emailed itself to user contacts after opened
"Code Red"	2001	$2.6 billion	1 million	Scanned Internet for Microsoft computers—attacked 100 IP addresses at a time
"My Doom"	2004	$38 billion	2 million	Emailed itself to user contacts after opened
Stuxnet	2010	Unknown	Unclear	Attacked industrial control systems
"Heartbleed"	2014	Estimated tens of millions	Estimated at 2/3 of all Web servers	Open Secure Sockets Layer flaw exposes user data

Sources: "Top 5 Computer Viruses of All Time," UKNorton.com, available at < http://uk.norton.com/top-5-viruses/promo>; "Update 1—Researchers Say Stuxnet Was Deployed Against Iran in 2007," Reuters, February 26, 2013, available at <www.reuters.com/article/2013/02/26/cyberwar-stuxnet-idUSL1N0BQ5ZW20130226>; Jim Finkle, "Big Tech Companies Offer Millions after Heartbleed Crisis," Reuters, April 24, 2014, available at <www.reuters.com/article/2014/04/24/us-cybercrime-heartbleed-idUSBREA3N13E20140424>.

New generation of malware: Super viruses + evolving, learning, adaptive, complex targeted attacks – new APTs)

New computing paradigms and technologies - cloud computing, the internet of things, big data, inmemory computing, blockchain

>> new playgrounds for malware authors to develop complex and sophisticated malwares

Relying on Kindness of Machines? **The Security Threat of Artificial Agents.**
By Randy Eshelman and Douglas Derrick. JFQ 77, 2nd Quarter 2015.

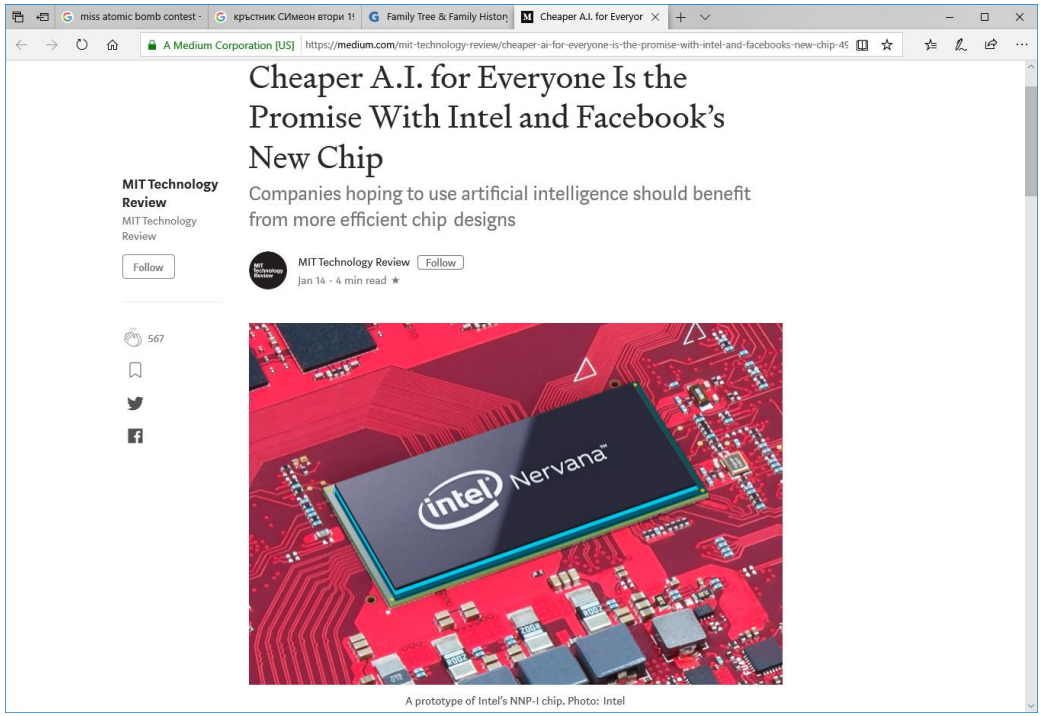
Weaponized AI used to develop new cyber attacks (new generation APTs) by:

- **Militaries** - cyber-weapons, super robot-soldiers, autonomous drones and precision lethal weapons
- **Governments** - use AI/ML to monitor/control people, or disrupt other states (governments, economy, society)
- **Corporations** – competition war-games, intel
- **Hackers** – steal, penetrate, destroy (ransom), “stealth” invisible activities (“as a service”)
- **Doomsday cults** attempting to bring the end of the world by any means.
- **Psychopaths** – appear in history books by any means
- **Criminals** – dark web and proxy systems for any unlawful activities

Accessible AI/ML as a Service - anyone could be bad actor!

Adversaries – access to cheap and powerful AI/ML tools

By the year 2021, cybercrime losses will cost upwards of $6 trillion annually.



Cyber/hybrid (cybrid) crisis?
Or constant low-level cyber war?

The Washington Post
Democracy Dies in Darkness

Opinions

The most damaging part of Trump's response to the Mueller report

Paul Nakasone, the director of th
Cyber Command, in Washington

By David Ignati
Columnist
May 30 at 5:55

community, has responded by developing a tough new doctrine to counter cyberattacks by Russia and other rivals. The premise is that our adversaries are engaged in constant cyberassaults against us and that the United States should adopt a strategy of "persistent engagement."

What this means, basically, is that the United States is now in a low-level state of cyberwar, constantly.

EXECUTIVE ORDERS

Executive Order on Securing the [nformation and Communications Technology and Services Supply Chain

INFRASTRUCTURE & TECHNOLOGY | Issued on: May 15, 2019

★ ★ ★

as
and

European Council
Council of the European Union

The European Council | The Council of the EU | Policies | Meetings | Documents & Publications | Press

Home > Press > Press releases

Council of the EU | Press release | 17/05/2019 | 11:52

Cyber-attacks: Council is now able to impose sanctions

On 17 May 2019, the Council established a framework which allows the EU to impose **targeted restrictive measures to deter and respond to cyber-attacks** which constitute an **external threat to the EU or its member states**, including cyber-attacks **against third States or international organisations** where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP).

Cyber-attacks falling within the scope of this new sanctions regime are those which have **significant impact** and which:

- originate or are carried out from outside the EU
- use infrastructure outside the EU or
- are carried out by persons or entities establishe
- are carried out with the support of person or ent

The EU and its member states are getting ready to be more resistant and to respond to cyber-attacks.

EXECUTIVE ORDERS

Executive Order on America Cybersecurity Workforce

ECONOMY & JOBS | Issued on: May 2, 2019

★ ★ ★

UNCLASSIFI

AI in wild (use)

- AI for advanced malware detection and protection
  - ML for fileless malware detection >>> examples
  - AI/ML for static and dynamic analysis for malware detection
- AI/ML-based monitoring and safety systems (for any type of ICT
- Cyber protection for AI applications – seems only AI/ML can monitor the AI-empowered systems – “Trustworthy AI” (EI Guidelines), DARPA XAI project
- AI for red teaming and exercises (if bad guys are using it…)

But also

- AI/ML empowered APTs, campaigns, cyber/hybrid war

A proof:BG-GB Cyber Shockwave exercise

“Skin in the game”

- Industry (Gas and oil distribution) >>> State (3 ministries, 3 agencies)
- Technical + Tabletop (4 main attack vectors + misinformation)
- Small (business) is BIG (threat)
- Context: EU elections (but CYBRID by nature, any time …)

Tested:

EU Blueprint (ENISA), Cybersecurity Incident Taxonomy, AI & ML pilot

Asymmetry demonstrated:

RED (+simple AI/ML) <> BLUE (Industry + State)

Result: 4 hours, score 3.5 for ??? out of 4

Supported by: UK Embassy, NCSC, UK companies/consultants

What’s next: Romania, Greece

“If you are not part of the solution, you must be part of the problem”

Attributed to: Eldridge Clever (1969); African proverb, others