Innovation in Cybersecurity

Dr. Eng. Adrian Victor Vevera
General Director
ICI Bucharest

We are in a cyber arms race

- We are in a continuous race to ensure cybersecurity

- This is a race that we are always on the verge of losing

- We are faced not just with cybercriminals, but also ideological actors and state-sponsored entities or actual states

- At the same time, we are in a race against the security implications of rising complexity in CI, cyber-physical systems and transborder infrastructures
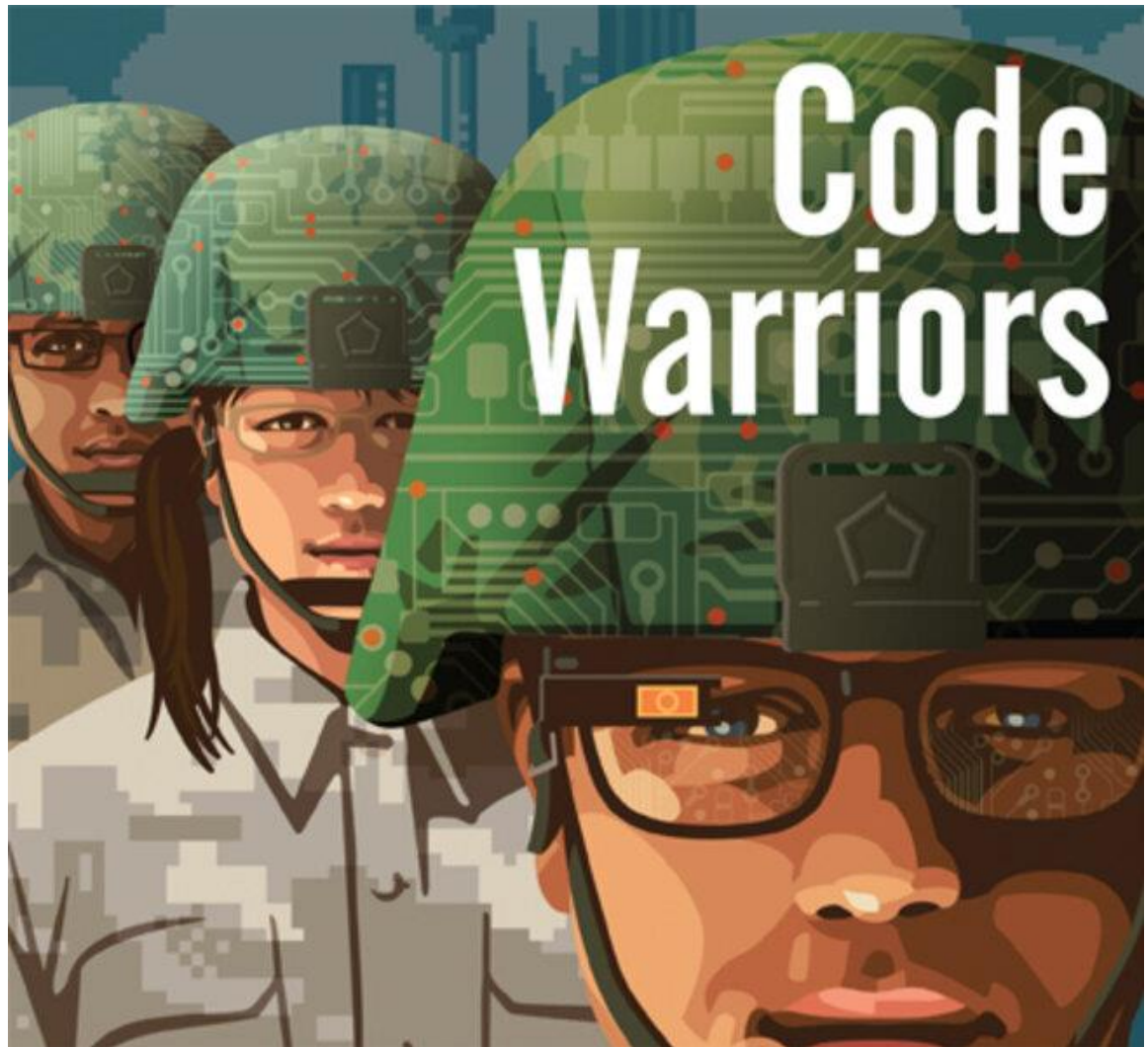
Complex Systems Challenges (Gheorghe et al, 2019) – everything applies to cyber systems as well

Human/Social
- Divergent Stakeholders
- Divisive Dynamics
- Conflicting Perspectives
- Ethical Conflict
- Generational Differences

Information
- Misinformation, Inaccurate
- Inadequate
- Incomplete, Inaccessible
- Proliferation, Overload
- Security/Privacy

Technology/Technical
- Rate of Change
- Obsolescence
- Complexity
- Incompatibilities
- Sociotechnical Concerns
- Affordability

Policy/Political
- Ambiguous Boundaries
- Excessive Maneuvering
- Demanding Constituents
- Emergent Conditions
- Divisive Power & Influence
- Irrationalities in Decision/action
- Defensiveness

Organizational/Managerial
- Shifting Demands
- Unstable Resources
- Unintended Consequences
- High Uncertainty
- Present-Future Focus Imbalance
- Solution Urgency
- Clarity of Purpose/Identity

How did we end up here

- The digitalization of life, society, the economy and politics
- Hybrid warfare and asymmetric warfare, including tactics such as state sponsored actors and proxies
- Targeting civilian infrastructure – banks, power generation and transmission, retailers, hospitals
- Transborder (dis)organized crime
- Global challenges related to networks, technologies, infrastructure, standards, regulations, conduct etc.
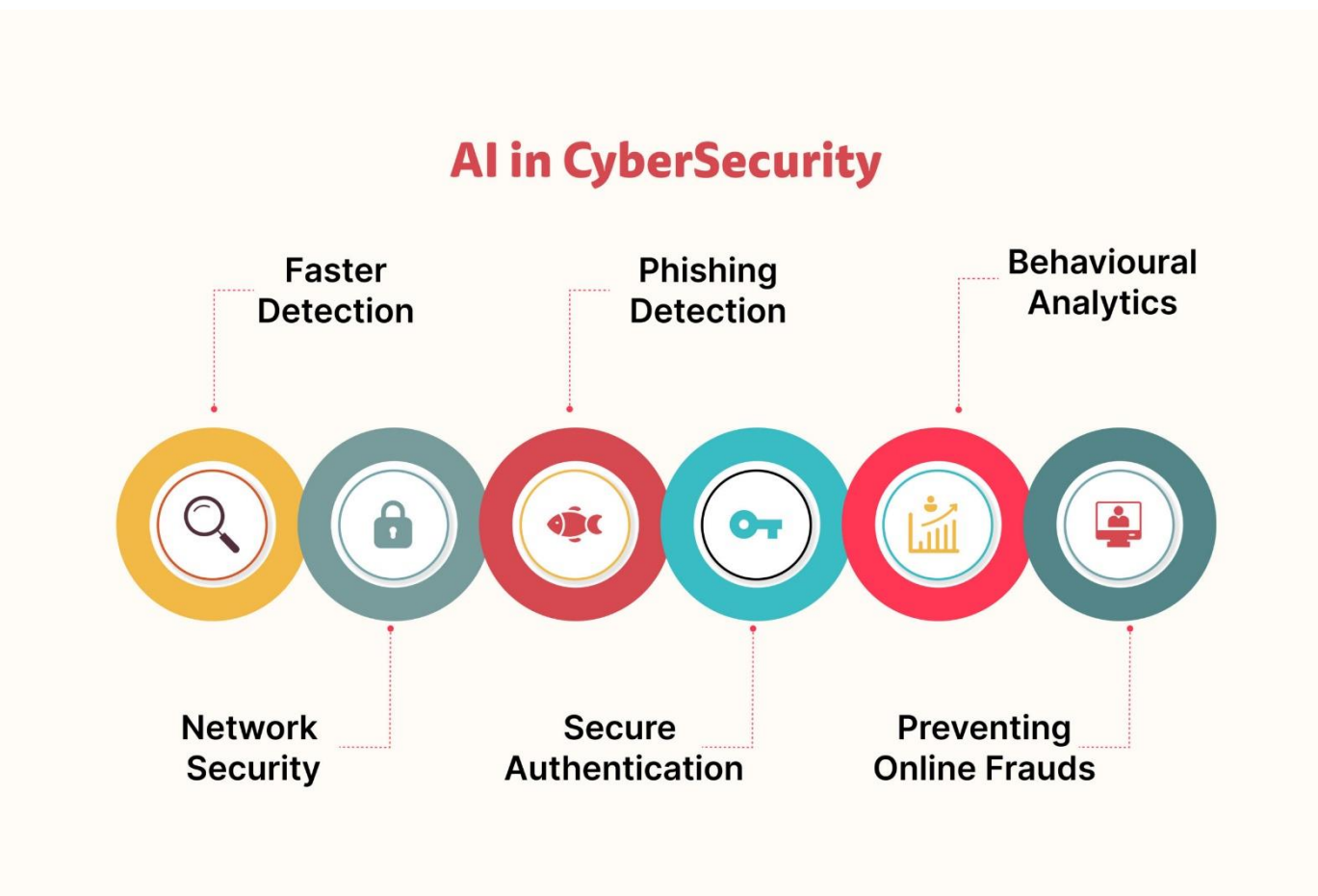- Emerging technologies rapidly being implemented for profit and efficiency

What is cybersecurity innovation about?

- The allocation of resources for cybersecurity purchases
- The pipeline for new products and services
- The pipeline and maturation rate for new technologies
- The possibility of the exchange of information, including in an automated way
- The development of cybersecurity culture as part of security culture in general
- Resilience by design in new critical infrastructures/critical entities
- A strategic culture that prioritizes cybersecurity
- Education that prioritizes lifelong training, competence certification and retention
- The deliberate reinforcement of strategic targets such as the Three Seas Initiative project
- Regional and global cybersecurity governance

1. Artificial Intelligence and Machine Learning

- AI can become a gamechanger in cybersecurity, both as defender and attacker
- These systems can analyze enormous amounts of data quickly, without the need for human oversight, making them ideal for identifying suspicious activity and defending against advanced threats.
- Cybersecurity professionals are already leveraging AI and ML to detect real-time cyberattacks, making their role even more important in maintaining a secure online environment.


AI in CyberSecurity

Faster Detection — Phishing Detection — Behavioural Analytics

Network Security — Secure Authentication — Preventing Online Frauds

2. Distributed ledger technology

- Provides a secure and immutable ledger of data to store critical assets

- Entities can can reduce their risk of cybercrime by inactivating record manipulation and unauthorized access.

- Multiple authentication steps are required for any changes to be made in a blockchain network, allowing for an enhanced level of distrust among users.

- Blockchain networks an effective tool for verifying identity, increasing data security, and preventing malicious data breaches.
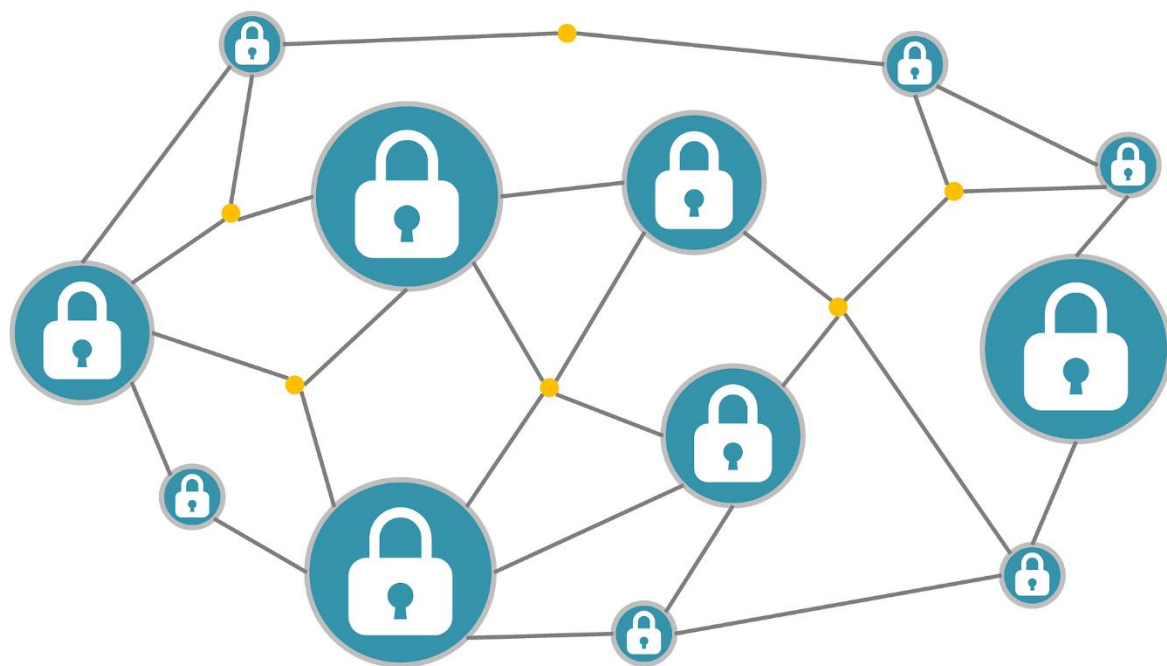
3. Zero-trust architectures
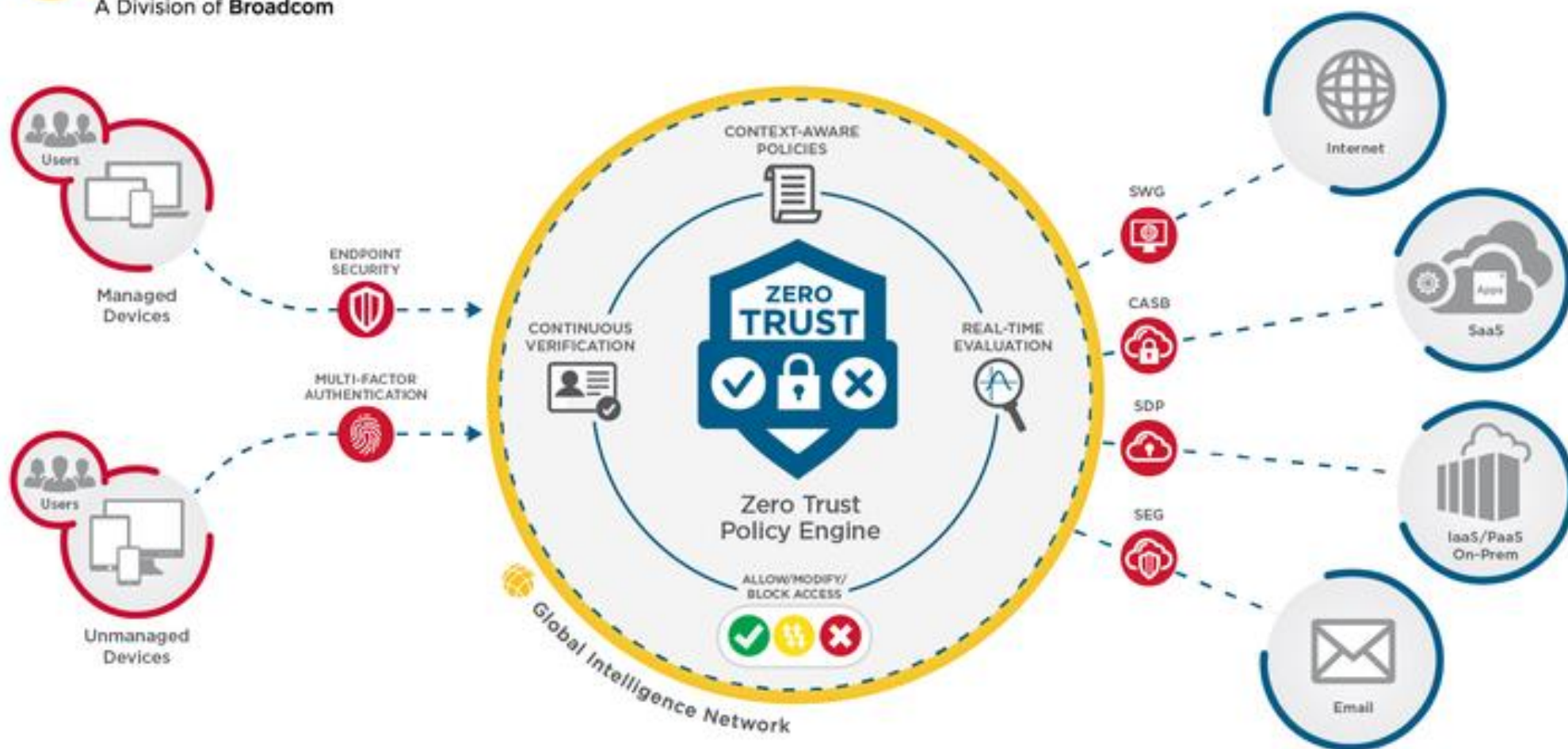
4. Behavioral Analytics

- This technology allows all behavioral data to be stored and then processed to examine trends, patterns and habits in each user's workflow.

- A behavioral baseline is created for the whole organization and when, for example, an abnormal increase in data transmission from a certain device happens, it indicates a possible cybersecurity issue.

- While this cybersecurity innovation was used for networks at first, it now shows an increasing application in user devices.

TOOLBOX™

IMPORTANCE OF NETWORK BEHAVIOR ANALYSIS

Puts enterprise data to work

Minimizes need for manual intervention

Reduces response times

Complements existing cybersecurity solutions

Deals with the latest threats faced by complex networks

5. Hardware Authentication

- Generates unique and temporary cryptographic code for users to type in alongside the password in order to gain access to stored data.
- This kind of approach relies on dedicated physical evidence for user authentication, in combination with a password.
- Physical security tokens can still be lost or stolen from legitimate users, but the scope is much lower for malicious interference.
- 2FA is something that is already widely adopted, while embedded authenticators as a technology for verification of user's identity are on the rise.

6. Do not forget Cyber Governance, through Cyber Diplomacy

THANK YOU

National Institute for Research and Development in Informatics - ICI Bucharest

Cybersecurity and Critical Infrastructure R&D Department
8-10 Averescu Avenue, 011455, Bucharest, Romania
office@ici.ro

WWW.ICI.RO