CYBER 2020

October 25-29, 2020
Nice, France

CYBER 2020

Introduction to Panel 3

Some of the Thematics to be discussed:

- Communications is an Essential Element of "Smart Systems"
- The Promise and the Peril of Emerging and Existing Communications Networks
- The Promise of Non-Orthogonal Multiple Access for 5G

Learning-based Space-Time Adaptive Processing (STAP)

- Leveraging Artificial Intelligence/Cognitive Computing to Meet the Increasing Cycles of Adaptation within the Cyber Domain
- Deep Reinforcement Learning for Attacker Agents and Defender Agents Autonomously Learning to Adapt to Counter these Attacks
- Polymorphic Agents as Cross-Sectional Software Technology for the Analysis of Cyber-Physical Systems

Thematics to be discussed (continued):

- There are well developed signature systems and concepts in other domains that can be well applied to cyber.
- Cognition of signature synthesis techniques and the finer points of analysis are critical skills.

Harmonizing the use of White box and Black box architectures to mitigate against machine learning bias

- Metacognition is becoming increasingly important as human and machine learning bias is becoming more evident.
- There are a variety of activities that are conducted in the physical, cognitive (social), and logical (cyber) realms with effects in the Information Environment (IE).

Thematics to be discussed continued:

- Are Legacy Devices common or rare?
- Is addressing these Legacy Devices easy or difficult?
- Are Legacy Algorithms common or rare?

Innovative Approaches for Contending with legacy issues

- Are Parametrics truly well understood? Are they understood accurately in the Information Environment?
- Prototype Architectural Stacks to explore the aforementioned…

WELCOME TO CYBER 2020

Panel 3!

Panel 3
Systems Resilience: Reliable Cyber-protection
(cyber defense, guaranteed reliability, cyber awareness, cyber-space, on-line cyber protection, traffic, …)

NexTech 2020

Chair

Steve Chan, Decision Engineering Analysis Laboratory, USA schan@dengineering.org

Panelists

Eric MSP Veith, OFFIS e.V. - Oldenburg, Germany eric.veith@offis.de
Ki-Hong Park, King Abdullah University of Science and Technology (KAUST), Saudi Arabia kihong.park@kaust.edu.sa
Joshua A. Sipper, Air Force Cyber College, USA jasipper@gmail.com
Xing Liu, Kwantlen Polytechnic University, Canada xing.liu@kpu.ca
Steve Chan, Decision Engineering Analysis Laboratory, USA schan@dengineering.org

CYBER 2020

Introduction to the Panelists

CYBER 2020

Panelist
Steve Chan

CYBER 2020

Panelist
Eric Veith

CYBER 2020

Panelist
Kihong Park

CYBER 2020

Panelist
Joshua Sipper

CYBER 2020

Panelist
Xing Liu

CYBER 2020

Introduction to the Research Interests/ Positions of the Panelists

Panellist Position

The Resiliency/Efficiency Nexus of Multi-Domain Cyber Convergence

Steve Chan, Decision Engineering Analysis Laboratory, USA schan@dengineering.org

- Strategic/Critical Infrastructure Protection
- Cyber-Physical Supply Chain Integrity
- Leveraging Artificial Intelligence/Cognitive Computing to Meet the Increasing Cycles of Adaptation within the Cyber Domain
- Monitoring and Evaluating the Cyber-health of Industrial Systems
- Advanced Analytics and Assessments

→ Discerning Blindspots at Multi-domain Interstices

→ Facilitating Blindspot Solution Discovery

About the Panelist

Panel, Nice, Oct 25-29, 2020

Eric MSP Veith

Manager of the research group *Power Systems Intelligence* at *OFFIS*, Oldenburg, Germany.
Likes to have Deep Reinforcement Learning agents compete for control of the power grid; researches AI-based modelling, analysis, and resilient operation of CPS. Lets the “attacker agents” learn attack trees to find weaknesses and loopholes in critical infrastructures, while “defender agents” autonomously learn to adapt to counter these attacks.
PhD in 2017, focusing distributed real/reactive power exchange with autonomous software agents. Is concerned with resilient criticial infrastructures since then.

Panellist Position

Safeguarding the Air in 5G/Beyond

Kihong Park, KAUST, Saudi Arabia kihong.park@kaust.edu.sa

- Physical layer security
- Optical wireless communication
- Unmanned aerial vehicle
- Non-orthogonal multiple access

5G cellular network and beyond

→ diversify spectrum, service, deployment, and device in networks

→ become more vulnerable to eavesdrop in the air

→ Be designed securely in a physical layer

→ With an emerging technology – FSO, UAV, and NOMA, etc.

About the Panelist

Dr. Joshua A. Sipper

Dr. Joshua Alton Sipper is currently assigned to the Air Force Cyber College (AFCC) as a Professor of Cyberwarfare Studies. He completed his Doctoral work at Trident University in September of 2012, earning a Ph.D. in Educational Leadership (emphasis, E-Learning Leadership). Dr. Sipper's previous degrees were obtained from Troy University (M.Ed. Education) and Faulkner University (B.S. English). Dr. Sipper is a veteran who served honorably in the U.S. Air Force in the intelligence career field, and worked for Lockheed Martin in a similar capacity on the U2 program. More recently, Dr. Sipper shifted his focus into the cyber realm as a Systems Engineer for General Dynamics at the Air Force's 26th Network Operations Squadron, followed by an eight-year stint as a civil servant in the Air Force cyber career field at the Curtis E. LeMay Center for Doctrine Development and Education. Dr. Sipper currently serves as a Professor of Cyber Warfare Studies at the Air Force Cyber College, Air War College, Air University, Maxwell AFB. Dr. Sipper's research interests include cyber ISR, policy, strategy, and warfare.

Panellist Position

Vulnerability of Cyber-Physical Systems

Xing Liu, KPU, CANADA, xing.liu@kpu.ca

- Story from a recently published article
- Wireless vulnerability
- Unencrypted and unsecured connections
- Firmware protection
- Weakest links
- Cyber security awareness

CYBER 2020

Questions & Answers Session

About the Panelist

Panel, Nice, Oct 25-29, 2020

Eric MSP Veith

Manager of the research group *Power Systems Intelligence* at *OFFIS*, Oldenburg, Germany.
Likes to have Deep Reinforcement Learning agents compete for control of the power grid; researches AI-based modelling, analysis, and resilient operation of CPS. Lets the “attacker agents” learn attack trees to find weaknesses and loopholes in critical infrastructures, while “defender agents” autonomously learn to adapt to counter these attacks.
PhD in 2017, focusing distributed real/reactive power exchange with autonomous software agents. Is concerned with resilient criticial infrastructures since then.

Panellist Position

Safeguarding the Air in 5G/Beyond

Kihong Park, KAUST, Saudi Arabia kihong.park@kaust.edu.sa

- Physical layer security
- Optical wireless communication
- Unmanned aerial vehicle
- Non-orthogonal multiple access

5G cellular network and beyond

→ diversify spectrum, service, deployment, and device in networks

→ become more vulnerable to eavesdrop in the air

→ Be designed securely in a physical layer

→ With an emerging technology – FSO, UAV, and NOMA, etc.

About the Panelist

Dr. Joshua A. Sipper

Dr. Joshua Alton Sipper is currently assigned to the Air Force Cyber College (AFCC) as a Professor of Cyberwarfare Studies. He completed his Doctoral work at Trident University in September of 2012, earning a Ph.D. in Educational Leadership (emphasis, E-Learning Leadership). Dr. Sipper's previous degrees were obtained from Troy University (M.Ed. Education) and Faulkner University (B.S. English). Dr. Sipper is a veteran who served honorably in the U.S. Air Force in the intelligence career field, and worked for Lockheed Martin in a similar capacity on the U2 program. More recently, Dr. Sipper shifted his focus into the cyber realm as a Systems Engineer for General Dynamics at the Air Force's 26th Network Operations Squadron, followed by an eight-year stint as a civil servant in the Air Force cyber career field at the Curtis E. LeMay Center for Doctrine Development and Education. Dr. Sipper currently serves as a Professor of Cyber Warfare Studies at the Air Force Cyber College, Air War College, Air University, Maxwell AFB. Dr. Sipper's research interests include cyber ISR, policy, strategy, and warfare.

Panellist Position

Vulnerability of Cyber-Physical Systems

Xing Liu, KPU, CANADA, xing.liu@kpu.ca

- Story from a recently published article
- Wireless vulnerability
- Unencrypted and unsecured connections
- Firmware protection
- Weakest links
- Cyber security awareness

Coping with the Unknown Unknowns

CYBER 2020 Panel

Eric MSP Veith <eric.veith@offis.de>

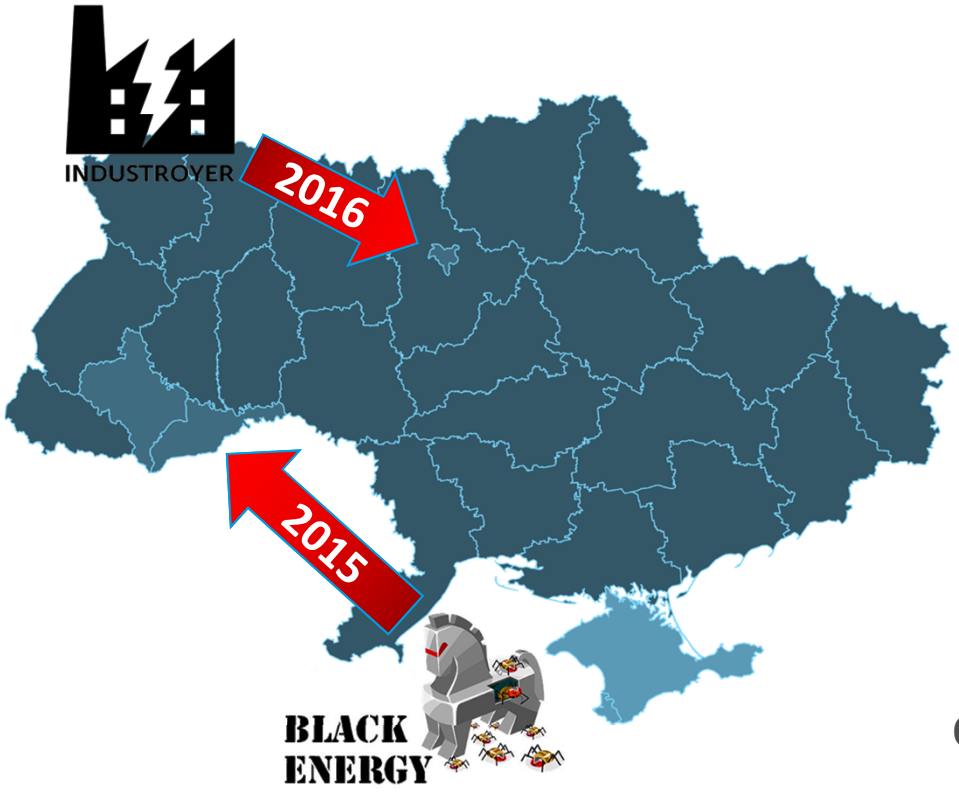
About the Panelist

Eric MSP Veith

Manager of the research group *Power Systems Intelligence* at *OFFIS*, Oldenburg, Germany.
Likes to have Deep Reinforcement Learning agents compete for control of the power grid; researches AI-based modelling, analysis, and resilient operation of CPS. Lets the “attacker agents” learn attack trees to find weaknesses and loopholes in critical infrastructures, while “defender agents” autonomously learn to adapt to counter these attacks.
PhD in 2017, focusing distributed real/reactive power exchange with autonomous software agents. Is concerned with resilient criticial infrastructures since then.

Applies to Critical Infrastructures, too

Attack against the Ukrainian Power Grid



Dec 23rd, 2015

- > Cyber Attack leads to **Blackout**
- > **3 Grid Operators** targeted
- > Operative **Intrusion into Control Systems**
- > Disconnect of **several Transformers**
- > Several Months in Preparation

2016

- > **Highly automated** Variant

Our infrastructures are valuable targets.

Learning & Adapting Attack Trees

Deep Reinforcement Learning for Autonomous Attacks

2016 Variant failed because it was automated.

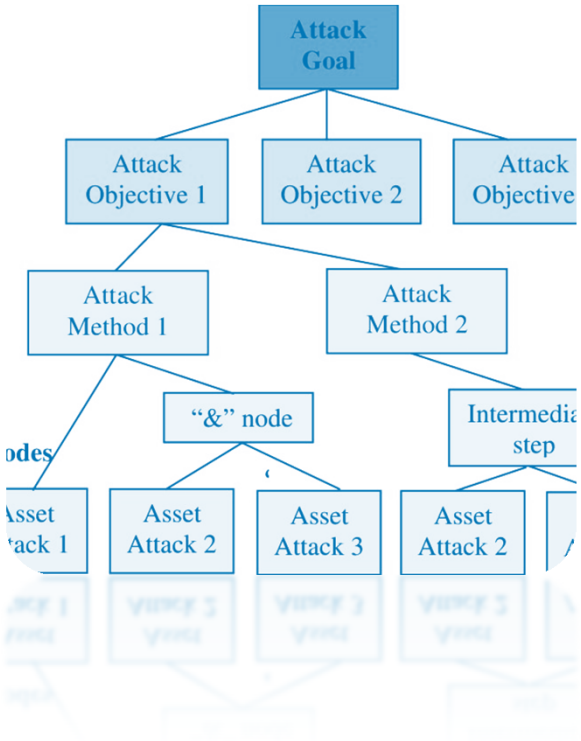
- Testing of the malware didn't account for a dynamic system.
- Attacks are still very much an interactive art:
  - There is no way of telling what one would encounter in a system.

Automation would strike like the proverbial bomb.

- Using AI to learn, vary, adapt attack trees
- Attacker develops strategies, adapts autonomously
- Attack trees reduce the search space.

This is not a weapon.

- These things will come.
- We need to have the defender ready.



Differentiable Neural Computer

Algorithm Approximation

ANN with external Memory

> John-von-Neumann architecture

> A differentiable computer, controlled by an Artificial Neural Network (LSTM)

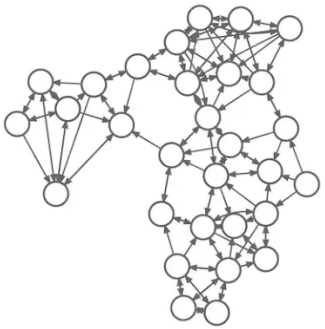
> Variable input-output vector size

Approximates Algorithms

> Learns to traverse and modify trees

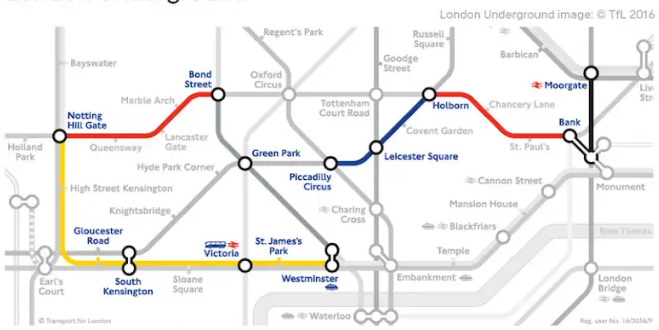
> Can learn on random trees, works on any other input and output tree.

Random Training Graph



Google Deepmind

London Underground



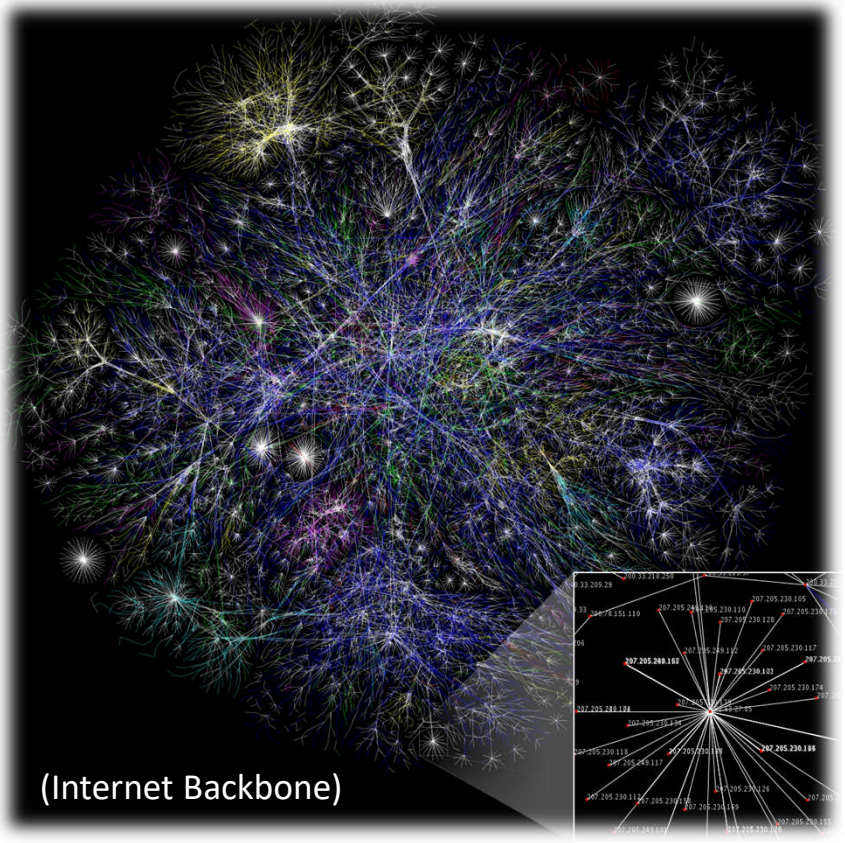
Traversal

Shortest

Learning Resilient Control

CPS inherently vulnerable

- Interconnected CPS have always attack surface **due to their inherent complexity**
  - Low latency of ICT and OT
  - High interdependence
  - Complexity in breadth and depth
  - Cricital Services as SPOF (DNS, BGP, *SCADA, SDL*)
- Learning Stratgies for **automatic issue mangement**

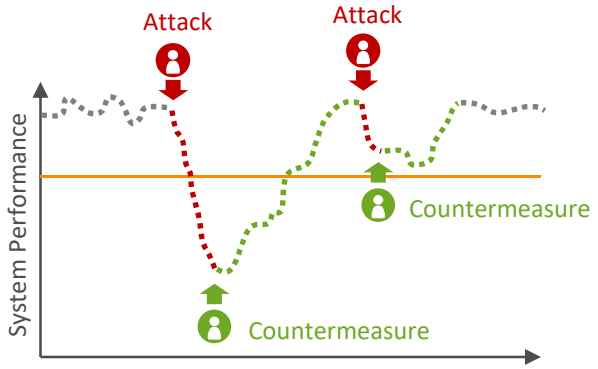


Adversarial Resilience Learning

Fully self-adaptive Agents analyze & learn Resilient Operation of the Power Grid

Two Agents Compete for Control of a Power Grid

- Self-learning, self-adaptive software agents
- Analyzer and Operator Agent compete for control, thereby training themselves
- No domain-knowledge: AI-based modelling of unknown systems

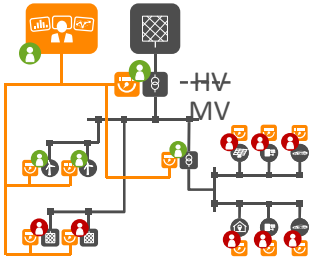


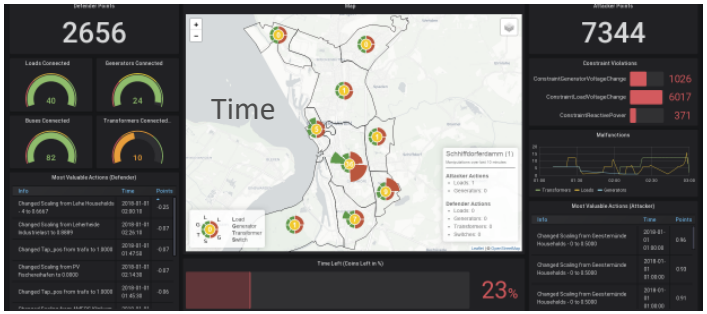
Preliminary Work

- PYRATE: Polymorphic agents as cross-sectional software technology for the analysis of the operational safety of cyber-physical systems

Faster Learning & Better Strategies: Many Opportunitinies

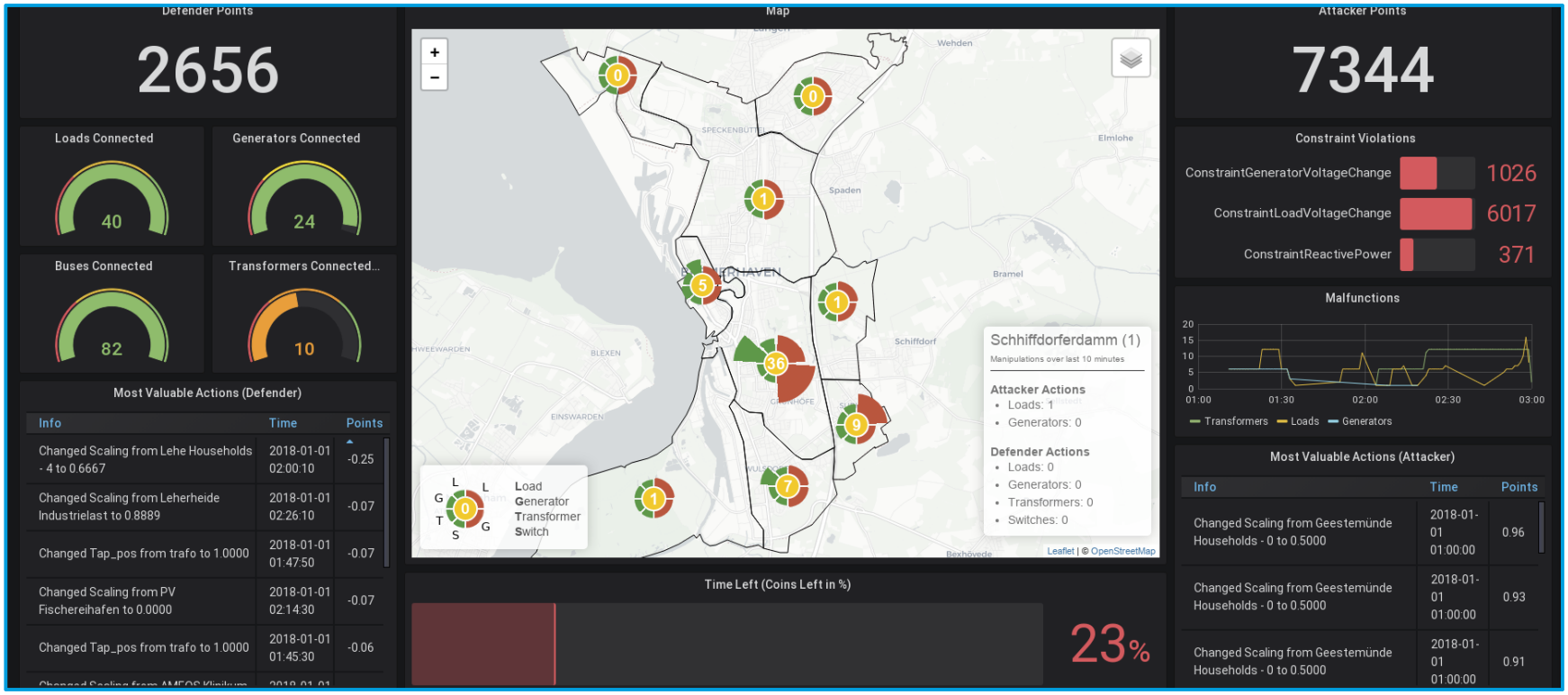
- Self-adaptive grid control
- Offer real resilience
- CO_2 reduction strategies
- Strategic grid planning





Power Grid Immune System

Flexibility comes from grid control, not from changing user behavior



NexTech2020
Panel 3 – Systems Resilience: Reliable Cyber-protection
Oct 18-22, 2020, Porto, Portugal

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Safeguarding the Air in 5G and Beyond



Kihong Park
Communication Theory Lab. @ KAUST
http://ctl.kaust.edu.sa

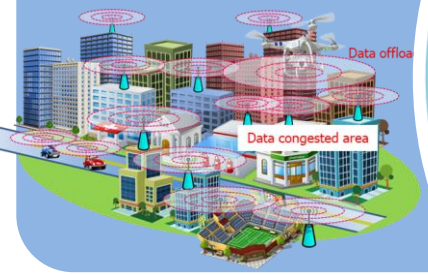
Network Diversification

5G User Cases with "Basic" Connectivity

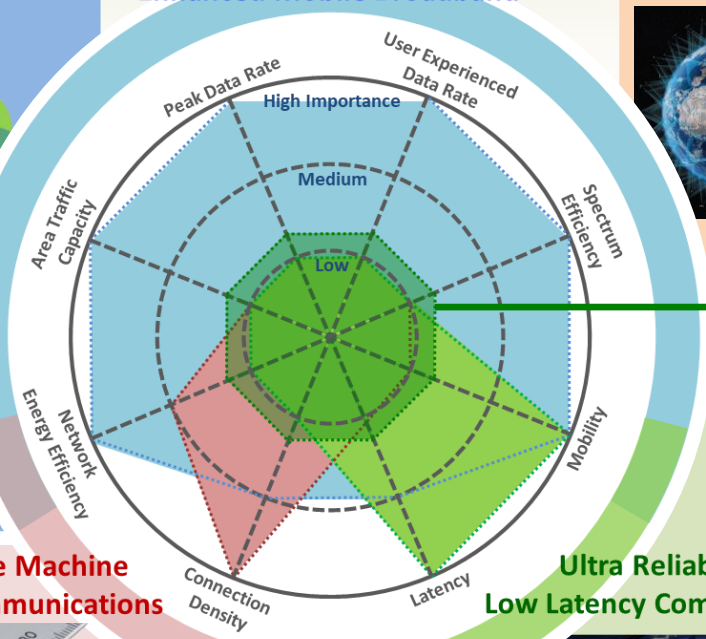
- *5G accelerates diversification in spectrum, services, deployment, and devices.*

Massive MIMO and mmWave

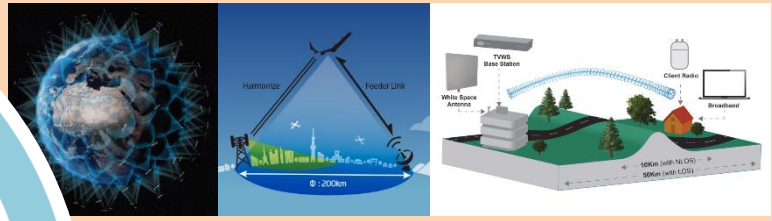
Network Densification



Enhanced Mobile Broadband



SATCOM HAPS TVWS



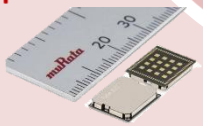
Basic Internet Access/ Global Access to the Internet for All (GAIA)

Drone-powered Solutions

Ultra Reliable and Low Latency Communications

Industrial IoT

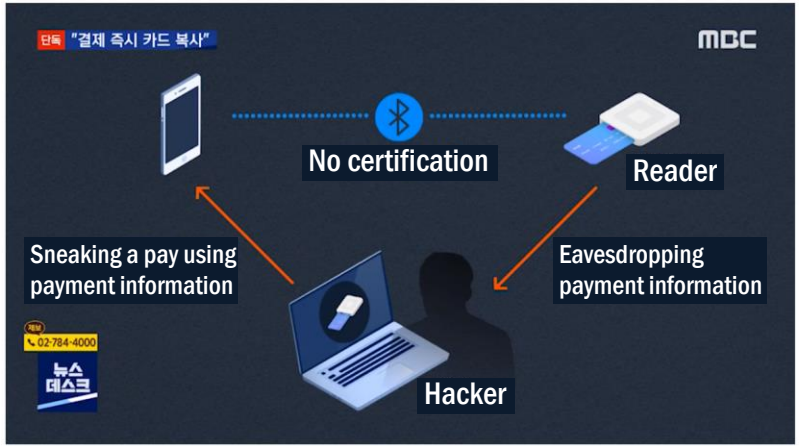
Massive Machine Type Communications



LoRa NB-IoT LTE-M sigfox

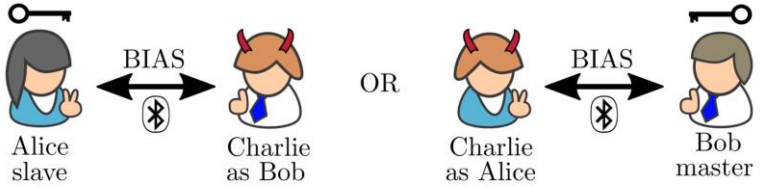
Weak Chain of Network - Security

- ***Some Bluetooth card readers can leak the card information.***



https://www.youtube.com/watch?v=X9oldMRLeuE

- ***Bluetooth Impersonation AttackS (BIAS)***
  - ***A severe vulnerability in the Bluetooth BR/EDR specification that allows an attacker to break the security mechanisms of Bluetooth for any standard-compliant device.***

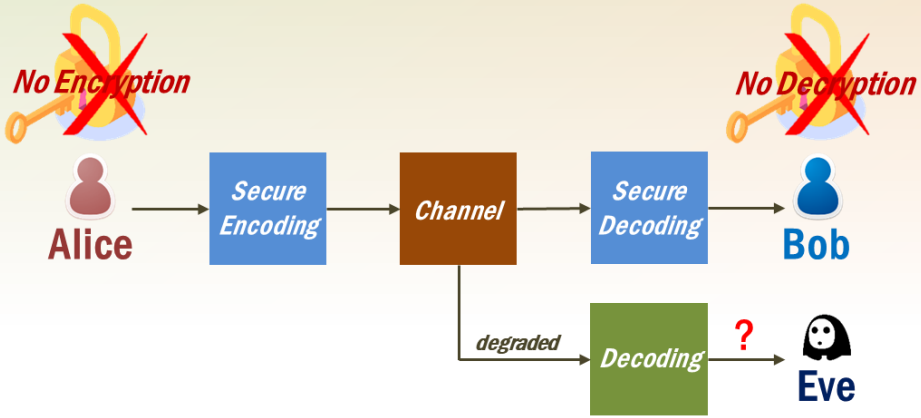


  - ***The research team conducted BIAS on more than 28 Bluetooth chips and all tested devices were vulnerable to the BIAS.***
  - ***Disclosed in Dec. 2019 and updated.***

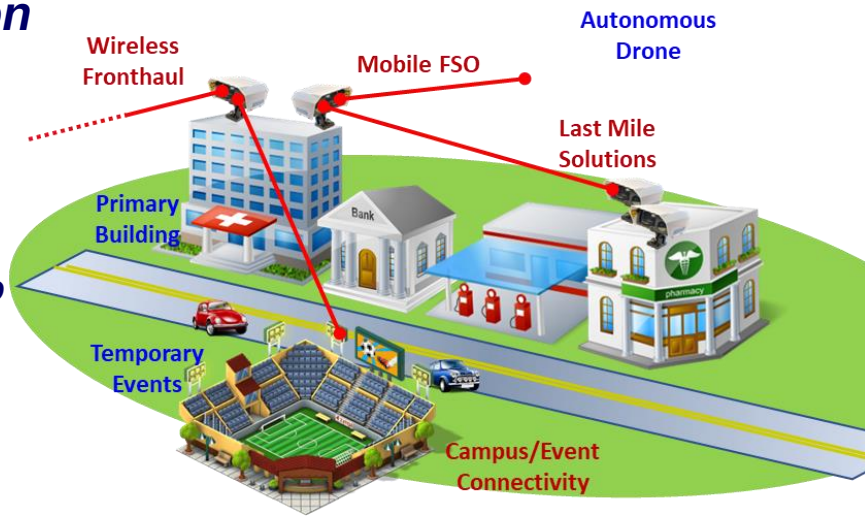
https://francozappa.github.io/about-bias/

Physical Layer Security

- ***In physical layer security (PLS),***
  - ***The transmitter sends a secure message to a legitimate receiver by taking advantage of inherent nature of wireless medium without the help of conventional encryption methods.***
  - ***Positive secrecy rate is guaranteed if eavesdropper channel is degraded.***



- ***Free space optical (FSO) communication***
  - ***Narrow beam connects two optical wireless transceivers in LOS.***
  - ***Unlicensed and unbounded spectrum***
  - ***Cost-effective***
  - ***Narrow beam-width (Energy efficient, immune to interference and SECURE)***
  - ***Etc.***

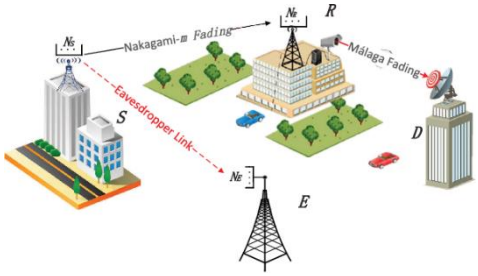


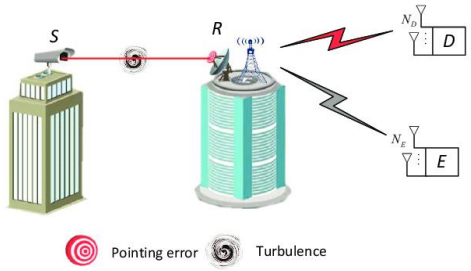
[1] M. Esmail, A. Raghed, H. Fathallah, and M. -S. Alouini, "Investigation and demonstration of high speed full-optical hybrid FSO/fiber communication system under light and storm condition", IEEE Photonics Journal, vol. 9, no. 2, February 2017.

Security in FSO Communications

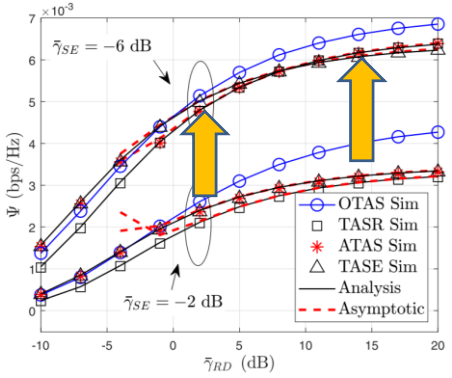
❑ Mixed FSO/RF systems

- *FSO link can be applied to wireless backhaul/fronthaul link in cellular network.*
- *By utilizing relaying technology, the mixed radio frequency (RF)-FSO systems combine both the advantages of the RF and FSO communication technologies.*
- *Thanks to the secure nature of narrow optical beam, the mixed RF/FSO relaying can offer better reliability in uplink/downlink.*

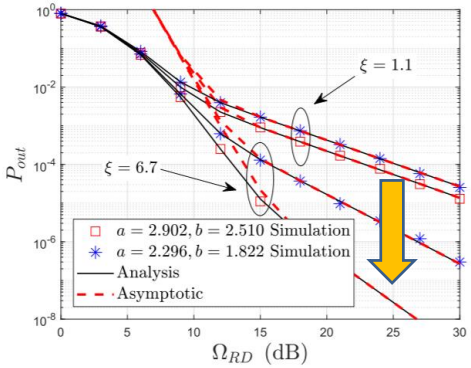




Mixed FSO/RF (Uplink)



Mixed FSO/RF (Downlink)

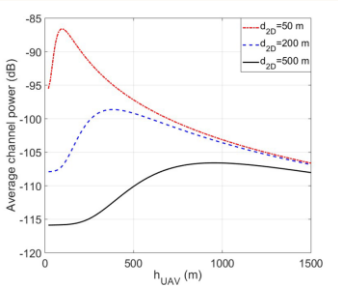


[2] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, M.-S. Alouini, "On secure mixed RF-FSO systems with TAS and imperfect CSI", appeared in IEEE Trans. Commun.
[3] H. Lei, Z. Dai, K.-H. Park, W. Lei, G. Pan, M.-S. Alouini, “Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems,” IEEE Trans. Commun., vol. 66, no. 12, pp. 6384-6395, Dec. 2018

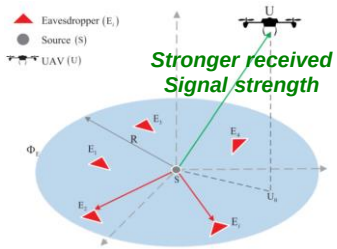
Security in UAV-assisted Communications

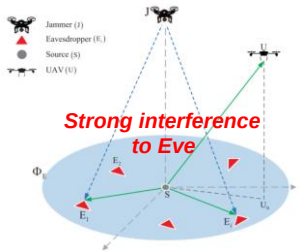
- ***Cellular-connected UAVs wirelessly exchange control and non-payload communications (CNPC) which should be ultra-reliable and secure.***

- ***The air-to-ground channel is altitude-dependent.***
  - ***Path loss exponent***
  - ***Line-of-sight (LoS) probability***

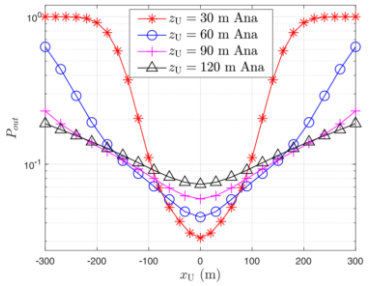


- ***Strong signal strength or severe Interference against ground and airborne users/BSs due to the LoS link.***





- ***By taking advantage of mobility of UAV, the PLS can be more reliable.***
  - ***The reliability of PLS is depending on the position of UAV in 3-D coordinate.***
  - ***For delay-tolerant information, the UAV transceiver can approach legitimate transceiver as closely as possible.***



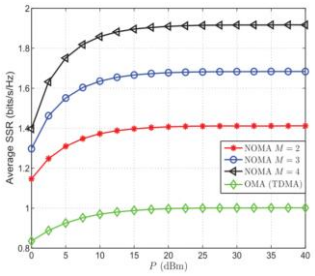
[4] H. Lei, D. Wang, K.-H. Park, I. S. Ansari, J. Jiang, G. Pan, and M.-S. Alouini, "Safeguarding UAV IoT communication systems against randomly located eavesdroppers", IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1230-1244, Feb. 2020.

Security in NOMA

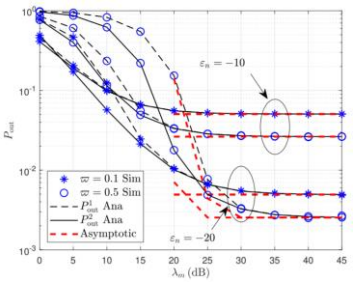
- ***Non-orthogonal multiple access (NOMA) scheme is an emerging technology for 5G networks to enhance spectral efficiency and massive connectivity.***

- ***In NOMA scheme, the signals of multiple legitimate users are superimposed.***
  - ***The multi-user interference degrade the signal reception at Eve and then the network secrecy rate/reliability can be improved collaboratively.***

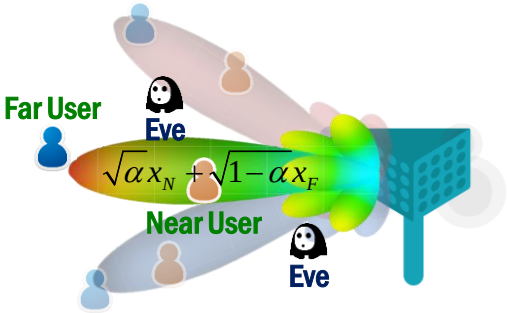
Rate



Reliability



- ***Directional beamforming with NOMA***
  - ***As the beam is narrowed down to a specific direction toward a legitimate NOMA user group, the secrecy sum rate will be enhanced.***
  - ***Power control and multi-beam precoding***



Secure precoding in NOMA-MIMO

[5] H. Lei, R. Gao, K.-H. Park, I. S. Ansari, K. J. Kim, M.-S. Alouini, "On secure downlink NOMA systems with outage constraint," appeared in IEEE Trans. Commun.
[6] Y. Zhang, H. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," IEEE Commun. Lett., vol. 20, no. 5, pp. 930–933, May 2016.
[7] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting interuser interference for secure massive non-orthogonal multiple access," IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 788–801, April 2018.


جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology
Thank You
ctl.kaust.edu.sa

ISR and EW Methods for Cyber Signature Development: A Conceptual Model

Dr. Josh Sipper
Professor of Cyberwarfare Studies
Air Force Cyber College
jasipper@gmail.com

IARIA

Biographical Sketch

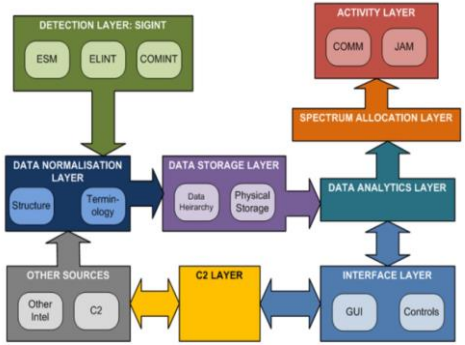
- Dr. Joshua Alton Sipper is currently assigned to the Air Force Cyber College as a Professor of Cyberwarfare Studies. He completed his Doctoral work at Trident University in September of 2012, earning a Ph.D. in Educational Leadership (emphasis, E-Learning Leadership). Dr. Sipper's previous degrees were obtained from Troy University (M.Ed. Education) and Faulkner University (B.S. English). Dr. Sipper is a veteran who served honorably in the U.S. Air Force in the intelligence career field, and worked for Lockheed Martin in a similar capacity on the U2 program. More recently, Dr. Sipper shifted his focus into the cyber realm as a Systems Engineer for General Dynamics at the Air Force's 26th Network Operations Squadron, followed by an eight-year stint as a civil servant in the Air Force cyber career field at the Curtis E. LeMay Center for Doctrine Development and Education. Dr. Sipper currently serves as a Professor of Cyber Warfare Studies at the Air Force Cyber College, Air War College, Air University, Maxwell AFB. Dr. Sipper's research interests include cyber ISR, policy, strategy, and warfare.

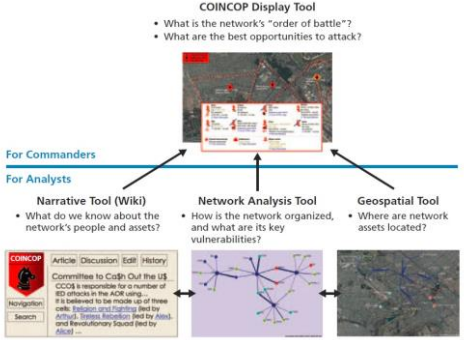
ISR and EW Methods for Cyber Signature Development: A Conceptual Model

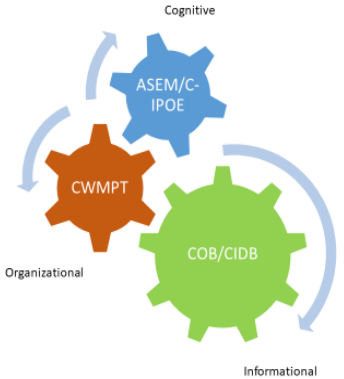
- Introduction
- Analytical Skills Education Model (ASEM)
- Cyber-Intelligence Preparation of the Environment (C-IPOE) Process
- Cyber Order of Battle (COB) Model
- Cyber Information Database (CIDB) Model
- Cyber Warfare Planning and Battlefield Management Tool (CWMPT) Model
- Cyber Signature Conceptual Model (CSCM)

Introduction

- Both of the information related capabilities of electromagnetic warfare (EW) and intelligence, surveillance, and reconnaissance (ISR) have very well-developed signature systems and concepts such as the Electronic Order of Battle (EOB) and Joint Intelligence Preparation of the Environment (JIPOE)
- The **Cyber Signature Conceptual Model (CSCM)** is a theoretical suite of tools that draws on EW and ISR constructs to suggest concepts and systems for cyber signature development

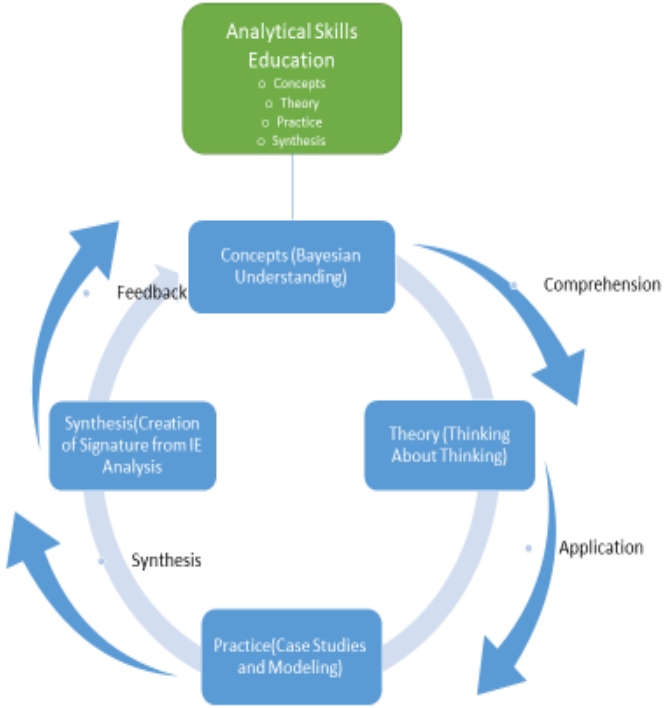






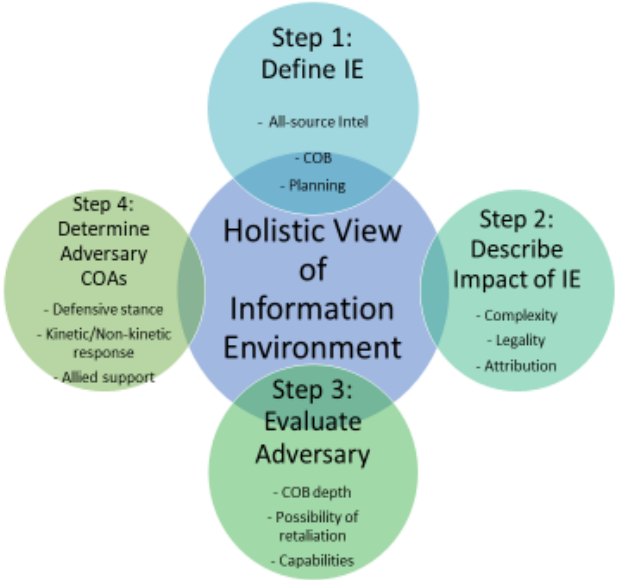
Analytical Skills Education Model (ASEM)

- Before analysis can be accomplished…must be educated in the finer points of analysis
- Conceptual alignment for all of the integrated parts is Bayesian Understanding
- Metacognition
- Practice
- Signature synthesis



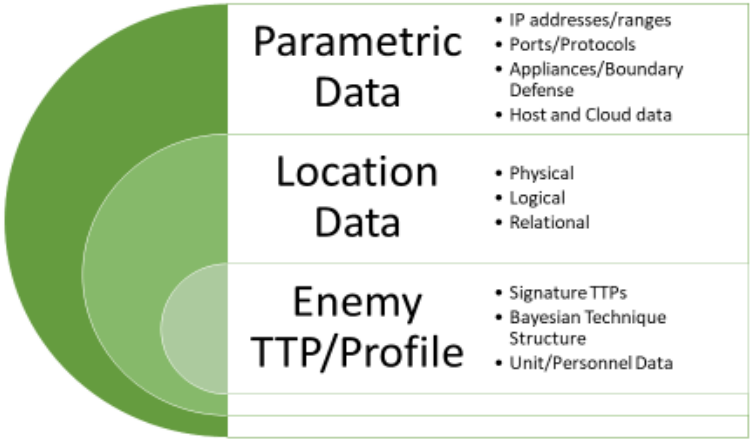
Cyber-Intelligence Preparation of the Environment (C-IPOE) Process

- Define the information environment (IE)
- Describe IE Impact
- Evaluate Adversary
- Determine Adversary courses of Action (COAs)
- All lead to a holistic view of the IE



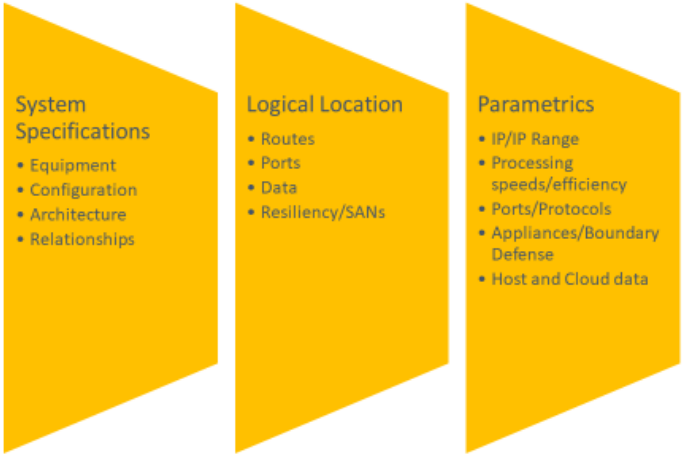
Cyber Order of Battle (COB) Model

- The COB is essentially a database including the necessary information needed for attribution and targeting
- Parametric Data
- Location Data
- Enemy tactics, techniques, and procedures (TTPs)/Profile



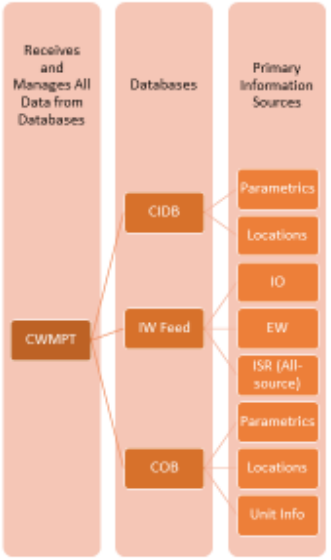
Cyber Information Database (CIDB) Model

- The CIDB is another database, but with much more granular data for specified targeting and cyber weapon development
- System Specifications
- Logical Location
- Parametrics



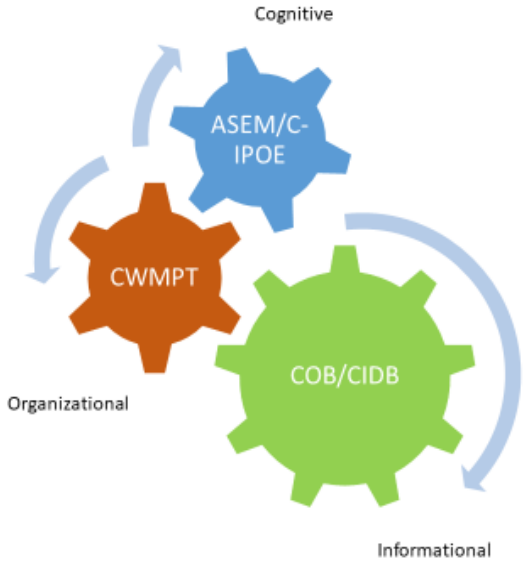
Cyber Warfare Planning and Battlefield Management Tool (CWMPT) Model

- The CWMPT is a central tool that brings information from all databases and is used for cyber operations planning
- Primary Information Sources
- Databases
- All-source Information Management



Cyber Signature Conceptual Model (CSCM)

- Finally, the CSCM is a high-level representation of the Cognitive, Informational, and Organizational gears that work together to give a full-spectrum, complete, and granular depiction of the IE for cyber signatures for attribution and targeting
- This is the full complement of numerous aspects of cyber information



KWANTLEN POLYTECHNIC UNIVERSITY

Cyber Attacks Originated from a Coffee Machine

- The lessons to learn from a published story

Xing Liu, Ph.D.
Kwantlen Polytechnic University, Canada
Email: xing.liu@kpu.ca

The Story …

- Came from this Forbes article:

https://www.forbes.com/sites/daveywinder/2020/09/27/hacker-takes-coffee-machine-hostage-in-surreal-ransomware-attack/?ss=cybersecurity#198ef2e377f0

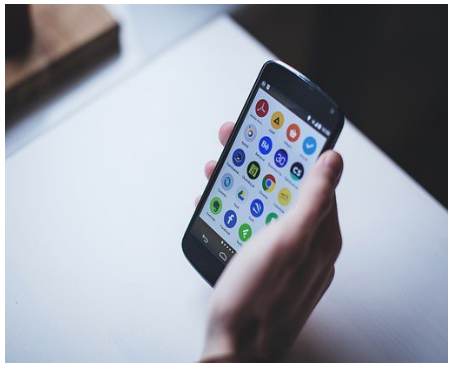
Sep 27, 2020

by Davey Winder, technology journalist

The Details …

- A researcher hacked a smart coffee machine without compromising the network or router
- The machine acted as a Wi-Fi access point, with an unencrypted, unsecured connection to a companion Android app
- Firmware update mechanism was unencrypted, without requiring authentication or code-signing

The Details … (continued)



The researcher:

- Reverse-engineered the firmware stored within the Android app
- Created a massive and noisy malfunction which can be stopped only by paying a ransom or pulling the plug
- Used a network connection command with malicious payload code that orders the coffee maker to demand for ransom
- The code also permanently turned on the hotbed, water heater, and the coffee grinder

The Details … (continued)

- Unplugging and reconnecting the machine does not solve the problem
- The coffee machine could be further programmed to attack the router or other network-connected devices
- The machine used was an older generation, no longer supported model

Here Is the Video …

- The hacked coffee machine “in operation”:

https://decoded.avast.io/wp-content/uploads/sites/2/2020/09/VID_20180828_185800_1-1.mp4

The Lessons and the Fixes?

My thoughts:

- Old devices: common or rare?
- Status of security of newer IoT devices?
- Challenges in implementing high-quality defence?
- State of art technologies and standards?