Defense Machines: Towards Autonomous Network Security Systems

Aman Singh
Palindrome Technologies
IEEE Symbiotic Autonomous Systems Workshop 2018
San Diego, USA

About Palindrome

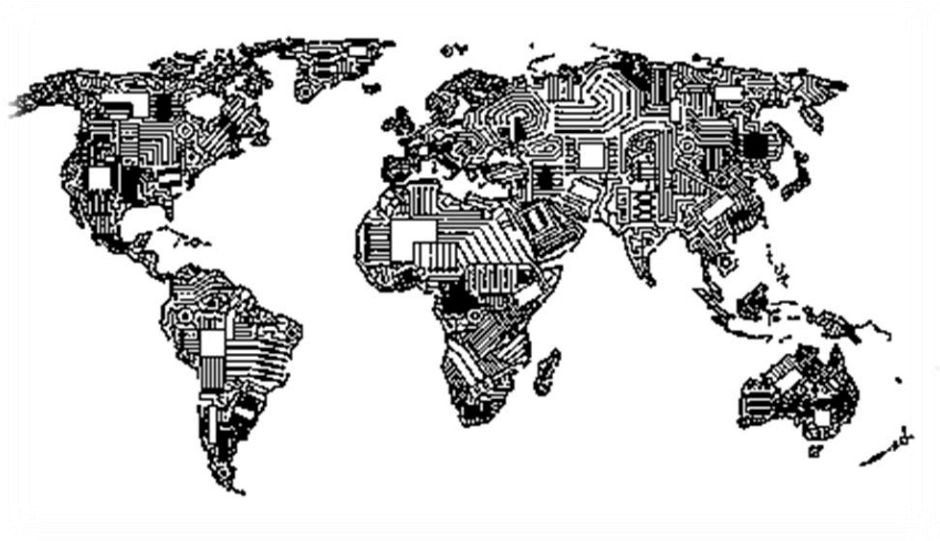
- Applied research lab, New Jersey
- Emerging technologies
  - Software-defined Infrastructure–5G/eUICC/Mesh HetNets
  - IoT - Security, Data storage
  - Blockchains
  - Machine intelligence - Content security
- Collaborative research projects*

Outline

- Internet Landscape
- Elements - IoT & AI
- Autonomous Security
- Conclusions

Q1

How will you describe the Internet landscape ?



1. Useless echo chambers
2. Land of Warlords
3. Useful uncertain medium
4. Necessary hostile land
5. Westworld 1.0

“Toxic Wasteland with *occasional* heavily defended citadels”

* Geoff Huston - https://blog.apnic.net/2018/06/25/looking-back-at-the-internets-past-decade/

Elements - IoT & AI

- Digitization of Society
- Automation of Processes
- Societal Networks
  - Healthcare
  - Agriculture
  - Manufacturing
  - Transportation
  - Government
  - ….

Q2

Autonomous Systems → Vulnerable Society

1. Yes
2. No
3. May be; need measurements
4. Yes; we can defend ourselves
5. Skynet is inevitable

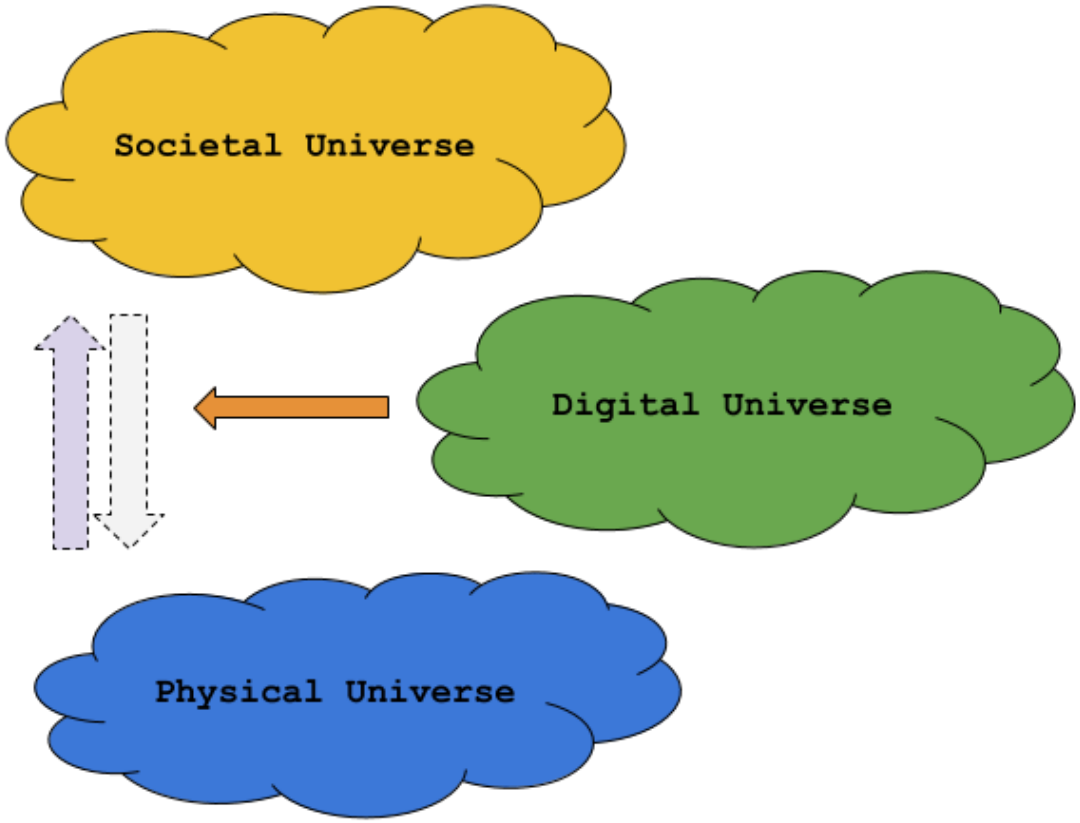
Technology Duality

- Email → Spam
- GPS → Tracking
- CCTV → Mass Surveillance
- Social Networks → Fake News Diffusion

Security Equilibrium

Defense →||← Offense

Impact Triad



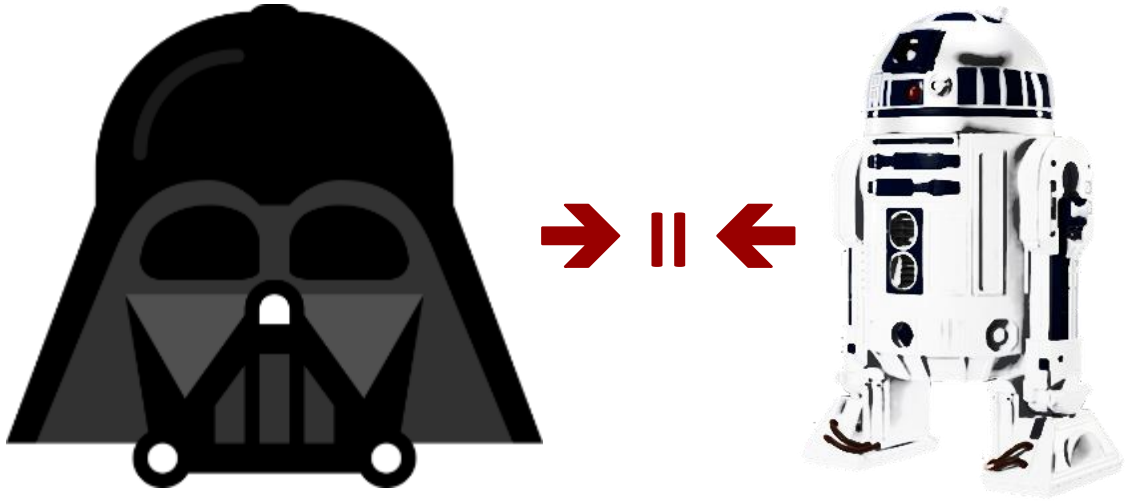
Offensive Autonomous Systems

- Digital Security
  - Social engineering attacks
  - Vulnerability discovery / attack pipeline
  - Human like DoS
  - Warfare– Bot vs. Bot
- Physical Security
  - Commercial systems for harmful attacks
  - Low-skill individuals with high-skill weapons
  - Increased scale
  - Warfare – Drones vs. Drones
- Political Security
  - Surveillance
  - Fake news – text / audio / videos
  - Personalized dis-information
  - Denial-of-Information Attacks
  - Warfare – Human vs. Human

* The Malicious Use of Artificial Intelligence: Forcasting, Prevention, and Mitigation, OpenAI, 2018

Q3

Autonomous systems equilibrium



1. 2028
2. 2049
3. 2100
4. Never

Attack Life-Cycle

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control (C2)
- Objective Actions

*Intrusion Kill Chain, E. Hutchins et. al, Lockheed Martin, 2011

Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Logs	**ACL**				
Weaponization	NIDS	NIPS				
Delivery	User/AV	Filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	Sandbox				
C2	NIDS	**ACL**	NIPS		DNS	
Objective Actions	Audit Logs			QoS	Honeypot	

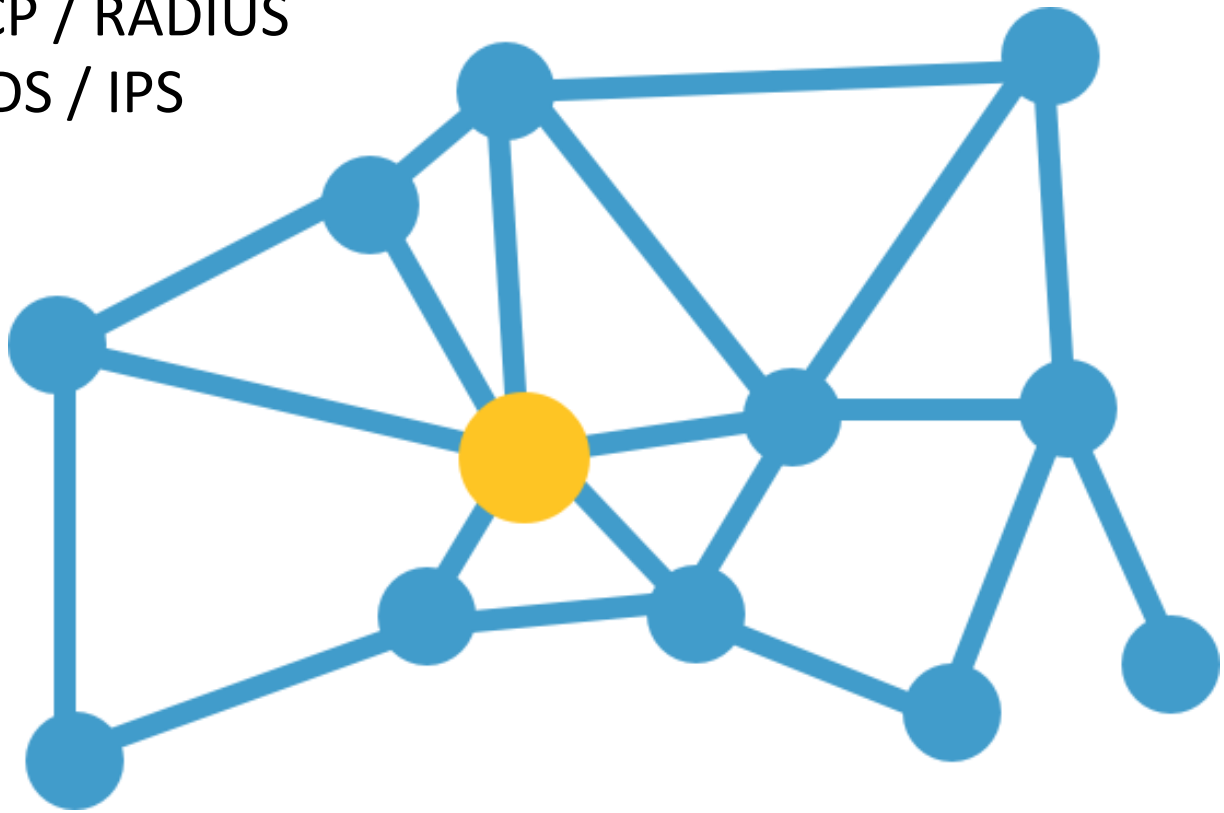
Defensive Autonomous Systems

Network-first Approach for Connected Things

*Joint work with – University of Luxembourg & Columbia University

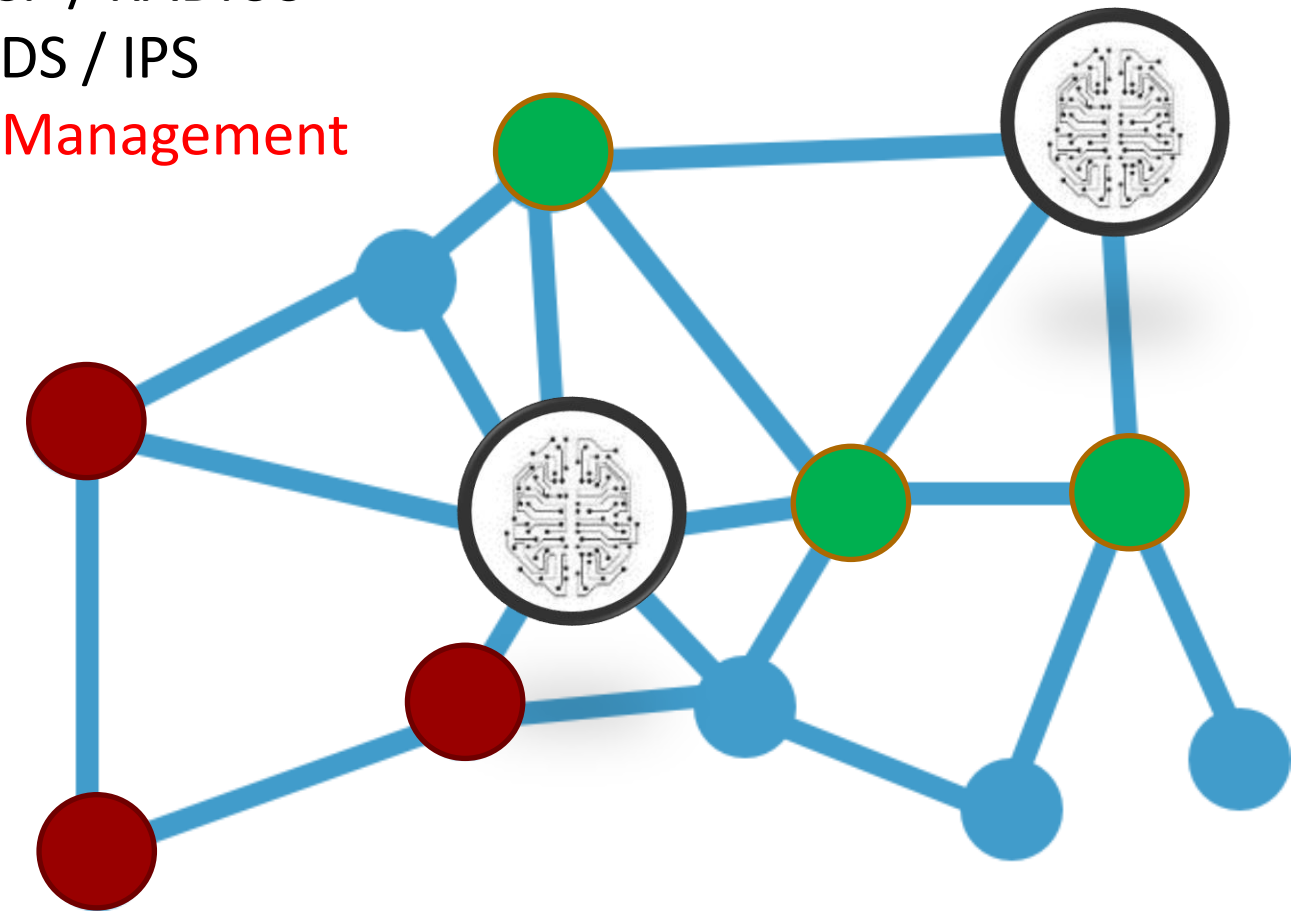
Network Elements

- Devices
- DNS / DHCP / RADIUS
- Network IDS / IPS



Network Agents

- DNS / DHCP / RADIUS
- Network IDS / IPS
- Life Cycle Management



Life-Cycle Agent

- Registration
- Configuration
- Operation
- Maintenance
- Quarantine

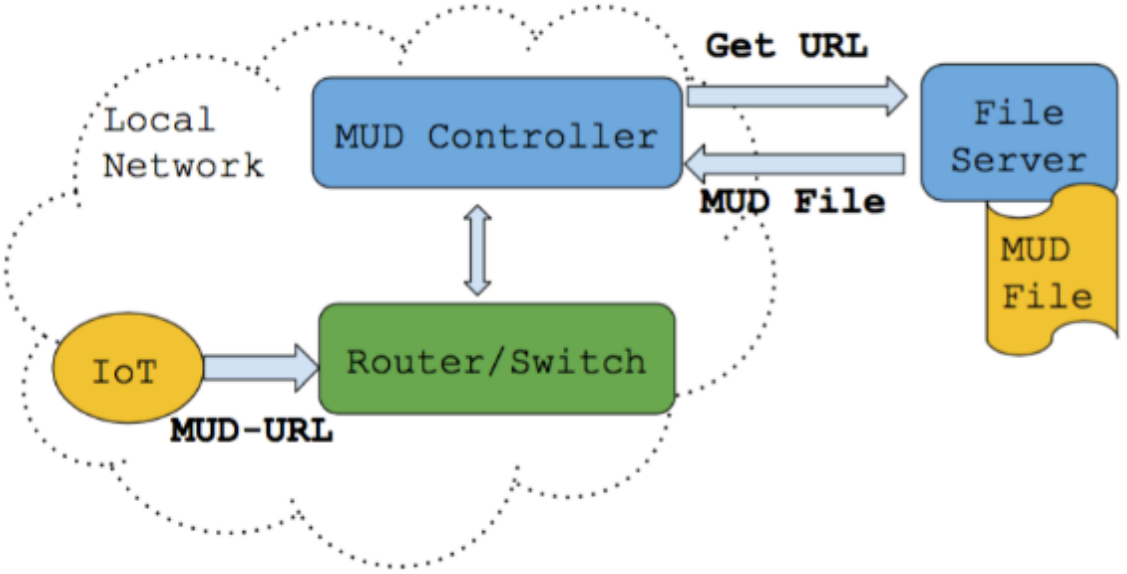
Insecure Things

- Vulnerable Default State
  - Software
  - Passwords
  - Protocol configurations
- Attacks
  - Mirai vs. Hajime
  - Cryptocurrency Mining
  - Crime Proxies
  - Ransomware
  - Data Theft
- Home vs. Enterprise

Good Things

- Limited functionality
  - Sense – Communicate – Actuate
  - Communication endpoints
- Device manufacturers
  - Management
  - Notifications

Manufacturer Usage Description



*https://tools.ietf.org/html/draft-ietf-opsawg-mud-25

HANZO* Controller

- Home Area Network Zero Operation (HANZO)
  - Autonomous Network Defense System
  - Devices, Profiles , Edges → Constraints
- MUD Profile by traffic observation

*https://en.wikipedia.org/wiki/Hattori_Hanzo

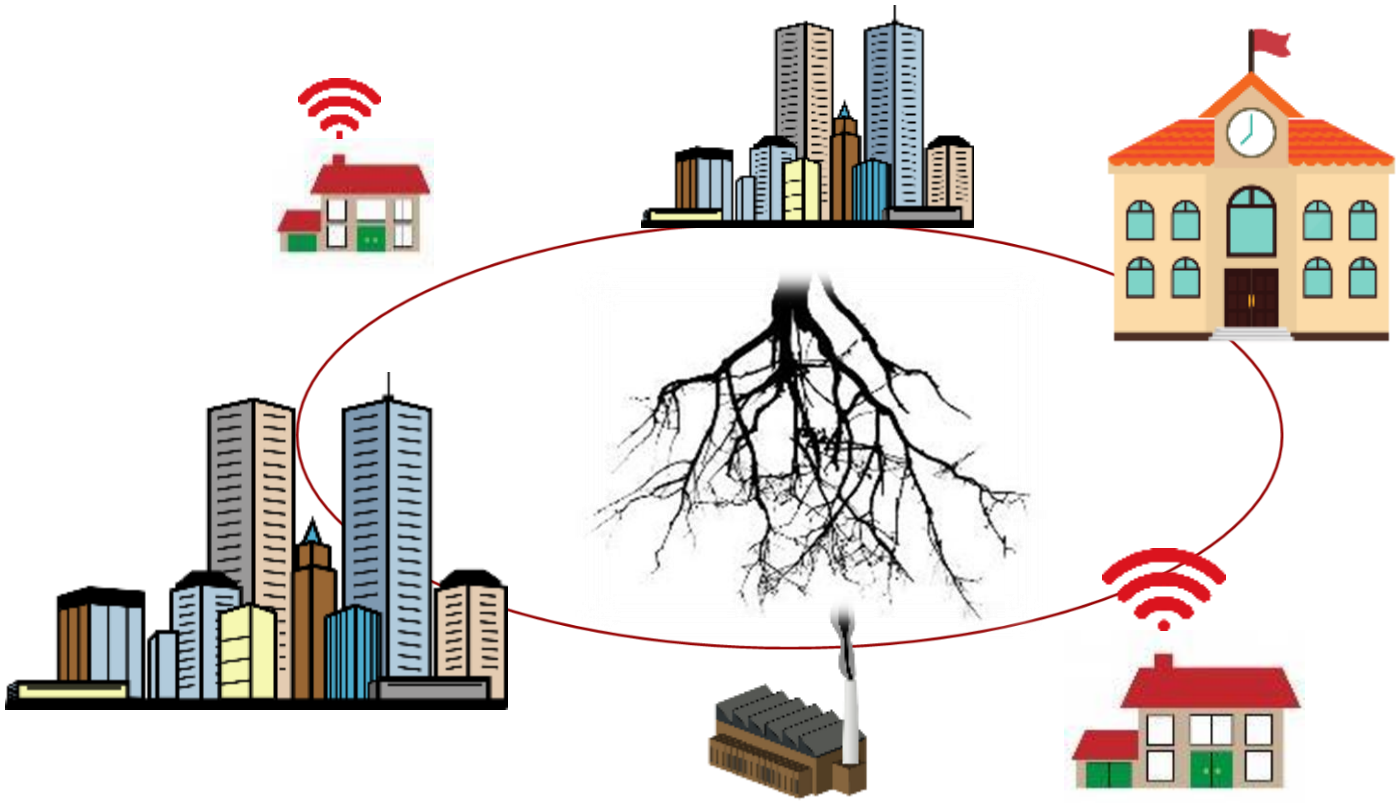
System Phases

- Monitoring
  - Metadata / default configuration
  - Endpoints
- Categorization
  - IoT vs General
- Generation
  - Device Profile
- Enforcement
- Continuous monitoring

Defense in Nature

- Mycelium Networks

Configuration Network



Q4

Configuration network management ?

1. Centralized Management
2. Peer-to-Peer Network
3. Hybrid model
4. Blockchains
5. Blockchains + AI

Test Automation

- Create Digital Twins
- System Data
  - Smart Home
  - Smart City
- Generative Adversarial Networks (GAN)
  - Function* (Input) → Output
  - Find best representation of F*

Interventions

- Hardware & Software
  - Formal methods
  - Automated testing / Fuzzing
  - Supply Chain
  - Vulnerability disclosures
  - Open source / Bug bounties
- Content Forgery Detection
- Consumer awareness

Conclusions

- Technology Evolution → Autonomous Systems
- Inherent duality - good vs. bad
- Need for better digital defense systems
- Need for better test systems
- Participation
  - Academia
  - Industry
  - Consumer
  - Government

References

1. The Malicious Use of Artificial Intelligence: Forcasting, Prevention, and Mitigation - https://arxiv.org/pdf/1802.07228.pdf

2. Towards Intelligent Autonomous Agents for Cyber Defense: Report on 2017 Workshop by NATO Research Group IST-152-RTG – https://arxiv.org/pdf/1804.07646.pdf

3. HANZO: Collaborative Network Defense for Connected Things, IPTComm 2018

4. Generative Adversarial Nets, NIPS 2014

Thank You

aman.singh [at] palindrometech.com