
**DYNAMIC POSITIONING CONFERENCE**
**October 09 - 10, 2018**

**Cyber Security Session**

---

# Cybersecurity – A Systems Perspective

**By Paul Mario Koola**

***Texas A&M University***

---

## Abstract

Cyberspace reaches all corners of human access and encompasses all interconnected devices into one large virtual entity. Cyber systems are complex adaptive systems that have interactions, linking individually based micro processes at the nodes to macrosocial outcomes at the network level. In such a system, even a perfect understanding of the individual parts does not automatically convey an ideal knowledge of the system's combined total behavior. Hence, complex critical systems such as dynamic positioning systems should be analyzed more holistically for cybersecurity vulnerabilities. These dynamic positioning systems are a fusion of information technology systems and operational technology systems known as cyber-physical systems. We argue that the lack of trust in information propagation is the key to a lack of robust security. We also opine that since humans control some cyber systems, these nodes of the network could have malicious activity as present in society. Creating an asymmetry for the malicious actor is one way to prevent penetration into the system and hence resulting attacks.

In this paper, we show that modeling such systems at different levels of resolution enable us to study the security properties of such systems more in depth, and generate metrics that can help us quantify the risk to potential vulnerabilities. We conclude by introducing some future technologies that might alter the cybersecurity landscape for cyber-physical systems such as dynamic positioning systems.

## Introduction

The Internet has enabled humankind to access all corners of our globe and even into space. Our connection to satellites in space has helped us to fix our position here on earth. These Global Navigation Satellite Systems (GNSS) such as GPS, GLONASS, Galileo, Beidou are satellite navigation or "satnav" systems. Each is an independent system of satellites that provide autonomous geo-spatial positioning with global coverage. This technology allows billions of small electronic receivers to determine our location (longitude, latitude, and altitude/elevation) on earth. This technology involves time signals transmitted along a line of sight by radio from these satellites. Jamming these time signals could force millions of users to lose their navigation capability. We take these systems for granted when we use maps to move from one location to another. Autonomous cars and ships depend on these navigation systems. Jamming all these time signals, across the globe, from every satellite, in each constellation is very difficult. A distributed spatially spread system is more challenging to take down entirely. It requires nation-state power to destroy most satellites in the constellation to make the system non-functional. Given that there are multiple GNSS, a robust technique would be to use various systems simultaneously to fix position in space. Dynamic Positioning (DP) systems have already taken advantage of this concept.

While global jamming or denial of service is difficult, local interference of all GNSS systems simultaneously is feasible, as the timing signals from the satellites tend to be in close electromagnetic range. Hence, DP systems tend to use non-commensurate sensors such as acoustic position fixing systems and inertial navigation systems, in addition to GNSS to ensure robustness of position fix. It is more difficult to hack into sensors, operating using different physical types (electromagnetic & acoustic) and produce the same make-believe erroneous signal from each of them. Our second observation is that using sensor fusion of non-commensurate sensors is more resilient to malicious hacking.

In this paper, we take a systems view of DP systems with a focus on cybersecurity. DP systems are Cyber-Physical Systems (CPS), which is the fusion of Information Technology (IT) systems and Operational Technology (OT) systems. IT systems encompass computing devices and networks with a design intent to store, process and transmit information securely. OT Systems are cyber physically networked systems that control the temporal behavior or dynamics of the system. The cybersecurity design intent for OT systems is to secure the dynamics of the system.

In the next section, we discuss cyberspace in general with the aim of understanding and securing DP systems.

## Cyberspace

Cyberspace reaches all corners of human access and encompasses all interconnected devices into one large virtual entity (Figure 1). Cyberspace in the maritime domain comprises ports and harbors, shipping, offshore facilities, and autonomous ships, and the satellites that keep these systems connected to the deepest depths of the ocean where autonomous underwater vehicles navigate. To understand the complexity and issues associated with cybersecurity, one must be knowledgeable about the evolution and growth of cyberspace.

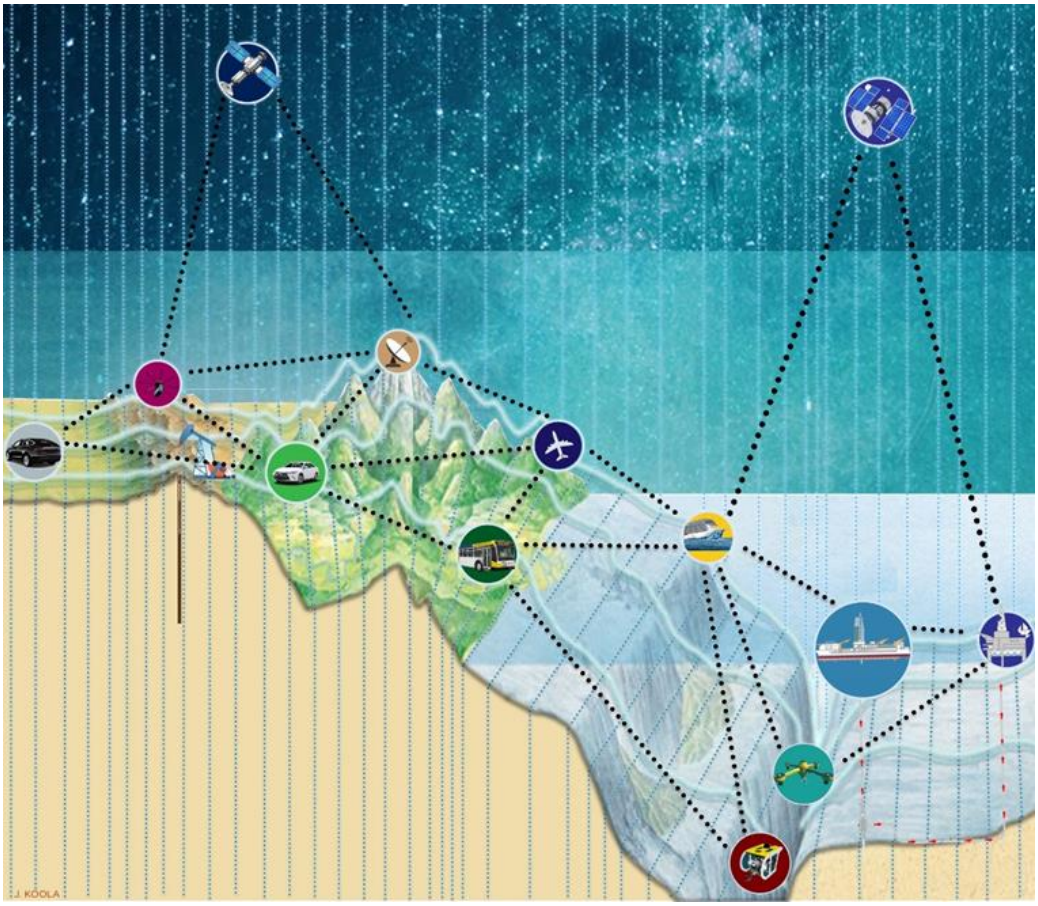

*Figure 1: Cyberspace – Devices Interconnected*

While cyberspace originally consisted of computer networks enabled with electromagnetic communications, IoT has enhanced this network with sensors and actuators capable of continuously monitoring and manipulating the environment we live in, transforming it into an ecosystem that has a life of its own. Given the pervasiveness of smartphones and other voice-activated gadgets integrated into this cyber network, the DNA of this network has human behavior in-built into it. Currently, we are in the era of man-machine symbiosis. Our societal push towards autonomous vehicles and the resulting expansion into the oceans is accelerating the rate at which the entire globe becomes instrumented, automated, and interconnected, giving us a first-look at real-time vision into every nook and corner. Acoustic communication with underwater robots further expand the electromagnetic medium to the acoustic medium and thereby extend our network reach. This complex adaptive system has lifelike behaviors due to dynamic manipulation of the nodes of this network by us humans. Cyberspace is mostly unregulated

and uncontrolled. We need to ensure that this system will not trigger unwanted consequences for the planet we live in, in this Anthropocene Age.

The Industrial Internet of Things (IIoT) has expanded IoT by combining industrial sensors and actuators with control to create complex, adaptive, networked systems. These CPS exchange information and propagate dynamic behavior across space and time. Cybersecurity enables securing this information transfer and dynamic behavior across CPS. Next, we discuss cyberspace as a complex adaptive system that needs to be studied more in-depth as we keep connecting more and more devices into this massive network without understanding the system level repercussions of doing so.

## Complex Adaptive Systems (CAS)

Cyberspace is a Complex Adaptive System (CAS). A CAS has interactions linking individually based micro processes at the nodes to macrosocial outcomes at the network level. In such a system, even a perfect understanding of the individual parts does not automatically convey an ideal knowledge of the system's combined total behavior (Miller & Page, 2007). These networks have self-organization capabilities (Figure 2 & Figure 3) and self-similarities like fractals. Flaws at the local nodes can replicate and produce emergent behavior at the global level. These facts help us engineer the system better, both at the micro and macro levels. Figure 2 is a flock of birds and Figure 3 is a school of fish. It is highly unlikely these biological entities understand the global pattern that each of them individually has created. When we keep adding more and more devices into cyberspace, we might be creating global patterns good or bad that we do not fully comprehend.


*Figure 2: Flock of Birds (Biber, 2018)*

*Figure 3: School of Fish (MacDonald, 2017)*

Human societies are also complex adaptive systems and each of us acting individually cannot easily see our global behavior as a population. Small individual plastic use by us humans gives rise to “The Great Pacific Garbage Patch” in the oceans. Similarly, greenhouse gas emissions give rise to climate change. It is difficult for us to see the impact we create globally. Some of these patterns help us understand the emergent properties of CAS. We still have not figured out the patterns we are building in cyberspace due to our behaviors.

We must dig deeper into the subsystems to help protect the cyberspace we have engineered. The subsystem behaviors at the nodes when aggregated produce the emergent properties at the systems level. It is hence useful to understand the subsystem nodes in more detail in the context of the overall system.

## DP – A System of Systems

Figure 4 shows the sketch of a DP system connected to other systems that interact with it. For this paper, we want to analyze this system as a set of nodes that are connected by links. Even though the DP ship is a system of systems, we can abstract it as a node. Some of the external links connecting into the DP System

are 1) GNSS with an error-correction reference-station for improved position resolution, 2) Communication satellite link through Inmarsat, 3) Acoustic underwater transponder signals for position keeping, 4) Weather inputs for environmental loading, 5) Helicopter and Offshore Vessels for personnel and food loading unloading and 6) Downhole data streams. The malicious hacker (cracker) can penetrate the DP System through any of these channels. The more sophisticated the cracker, the more channels they can penetrate simultaneously. Their goal is to control both information flow and the dynamics of this system. As we saw with CAS the more the nodes and their computational and control capability the more complex their behavior which is influenced by external disturbances. These disturbances could be environmental or maliciously triggered to cause harm.

General cracker strategies including jamming or crashing to prevent operation or spoofing where signals are altered but kept believable to cause more harm downstream. Spoofing is an order of magnitude more difficult than jamming but gives the adversary time to hide their tracks and get into the system and spread chaos, eventually to prevent the system from operating.

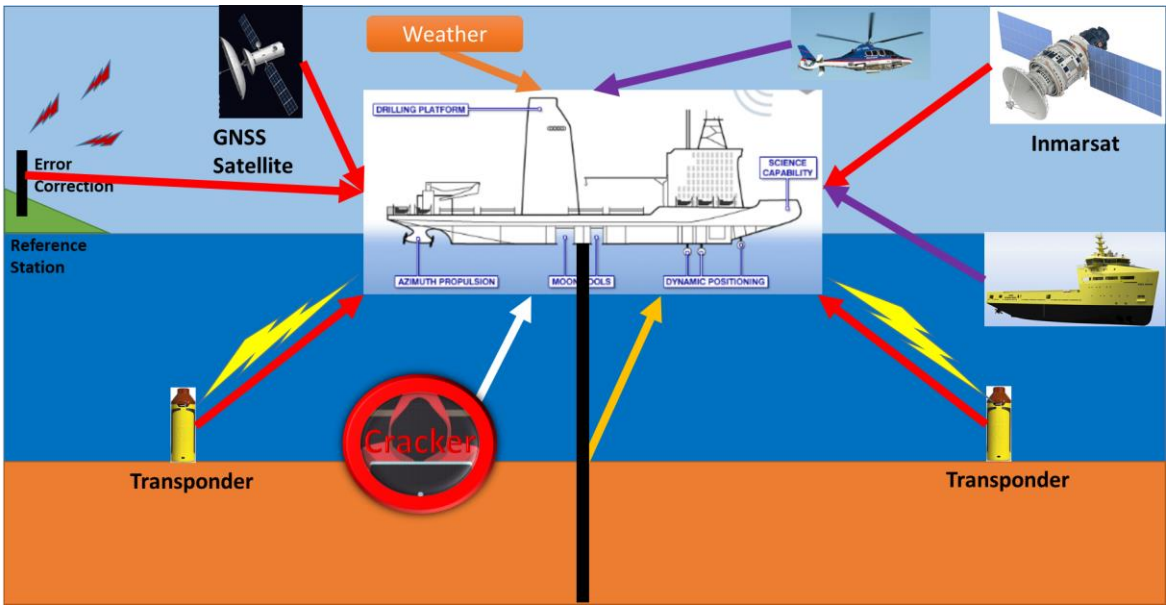


*Figure 4: Dynamic Positioning System – A System of Systems Network*

In the context of DP systems, we analyze the nodes and links in this network as generic abstractions with an aim to model and understand the system performance subject to disturbances and attacks.

## Subsystems & Trust

Just as every node on the human network is an intelligent human, we can model every generic DP subsystem node as a smart computation and control device with sensors and actuators. The human brain is the computational mechanism, our five senses sight, touch, hearing, taste, and smell are the sensors, and our limbs are the actuators. These nodes are a close replica, analogous to an individual on the human network. Not all nodes need to have all the capabilities of sensing, actuating, or even computation. In DP, computation at the nodes uses sensor feedback to control actuators and is analogous to the human body where the brain uses the senses networked together to control our limbs.

Given this abstraction, we can further reduce the subsystem node to a stack of components layered one on top of another. To keep matters simple and for this paper, our computational and control node consists of high-level parts where we can study security in more depth. This computational and control node comprises of the Hardware, Operating System (OS) and Application Software sitting on top of the

Operating System. We can add sensors and actuators as additional components, to the computational and control stack if so desired, without loss of generality. The sensors measure the environment, and the actuators react to the environment, based on the computation and control at the node.

Depending on the functionality, these nodes are sometimes classified as clients or servers. A node that produces information is a server and one that consumes information is a client. In bi-directional networks, both nodes could act as clients and servers. A GPS satellite for consumer applications is a server while the GPS device is a client. A GPS satellite can be degraded for defense applications, and it then acts as a client receiving inputs. In general, as the node is more capable and more complex, there is potential for more flaws. We have to manage security flaws for this explosion of capability.

Just as the nervous system in our body connects our brain to the various senses, we need channels of communication wired or wireless to connect the different nodes in cyberspace. Human senses communicate with nerves wired through our body to the skin for touch and tongue for taste and wirelessly through acoustic speech for hearing, electromagnetic visible spectrum for sight and chemical scent through the nose for smell.

As these networks grow in size and power, trust between nodes has become an issue. When we operated in small networks such as tribes, the chief knew and trusted all individuals and nodes that were not reliable were eliminated. The removal of some nodes maintained the integrity of the tribes. As tribes became societies and the network grew, new structures had to be put in place, like formal laws and courts to eliminate adverse behavior to control chaos and maintain the stability of the system. When people networks expanded to computer networks with humans controlling these nodes, we did not create a decent enough system to deal with trust at the nodes. The internet communication protocol was designed to propagate information from node to node irrespective of the damage to the other nodes in the network. As long as there is one path open between the two communicating nodes, the message will be passed, though there is no guarantee on the time it would take. Then communication was assumed to be between trusted parties and hence security was not a design intent. Cybersecurity issues we see today are due to the lack of trust between nodes. Trust in this network is the missing link that prevents us from securing this network.

Now that we have a base understanding of the nodes in the network and the communication channels connecting them and understand that lack of trust in this system is the reason for cyber-attacks, we can study how to model cybersecurity to understand attack possibilities to prevent them.

## Modeling Cybersecurity

Why is security so hard? It is because security is a negative goal (MIT xPro Cyber).

A bit of explanation might help understand this better. A positive goal is where we can verify the satisfactory completion of the goal, once the job is done to specification. If we were asked to prove if someone could take control of an ocean-going vessel, we could demonstrate that by someone authorized to do so and verify that we are satisfied with the result. A negative goal is to prove that an unauthorized person could never take control of the vessel. The burden of proof that an unauthorized person can never control the vessel as the number of possibilities increases gets more difficult.

Since the number of possible attacks is infinite, it might be a better strategy to model cybersecurity, and then the model can be tested for all possible attacks that one can strategize. These models can also help improve security by design before actual systems are physically built.

Cybersecurity models can be built at different levels of resolution (Figure 5). Modeling is an art and always involves trade-offs between accurate representation and computational load. The number of attributes versus the level of details represented by each attribute plays a role in determining what resolution of the model is required.

Next, we study three different modeling paradigms to understand the differences.

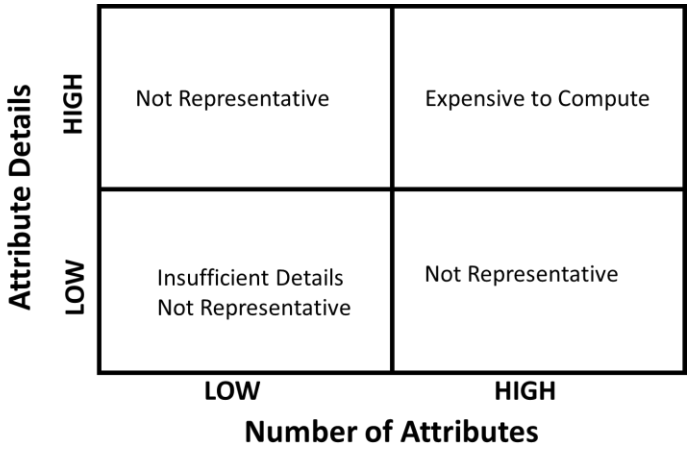


*Figure 5: Model Resolution*

1. *High-Level Model - Virus on a Network*

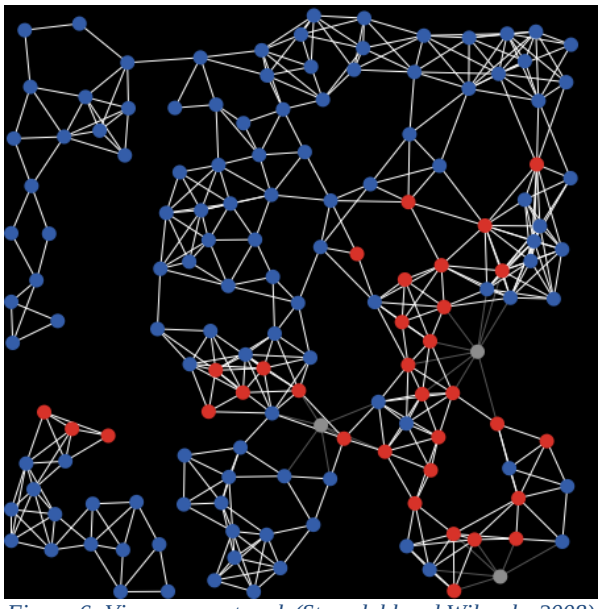

*Figure 6: Virus on a network (Stonedahl and Wilensky 2008)*

Figure 6 shows a system level simulation model of virus propagation (Stonedahl and Wilensky 2008). These high-level simulation models can span across domains from disease propagation to computer virus spread and help us understand and operate these systems better. The spread of disease like flu across the human population is studied in Epidemiology. Vaccination as a mechanism to prevent the spread of the disease-causing bacteria or virus (Honner, 2018) has an analog on a computer network similar to an antivirus software deployed on the network's node machines. These network effects modeled at the global

system level and the impact of virus propagation are studied based on three states: Susceptible, Infected, or Resistant referred to as an SIR model for epidemics.

These models can answer questions such as how many nodes need to be resistant for a given network topology to prevent the spread of the virus that could bring down the whole network. There are certain thresholds of resistant nodes above which the virus cannot spread throughout. It would be informational to understand these system parameters.

### *2. SysML To Graph-Based Model*

The Systems Modelling Language (SysML) is a general-purpose modeling language for systems engineering applications that support the specification, analysis, design, verification, and validation of a broad range of systems and systems-of-systems. Cyber-Physical Systems such as DP can be modeled in SysML but to carry out cybersecurity analysis it is best to convert them to graph structures with nodes and links corresponding to chosen attribute relations between nodes as shown in Figure 7 for a Flight Control System (FCS) (Bakirtzis et al. 2018). As can be seen in the graph representation of the system each node represents a hardware component with links representing communication protocols or action.

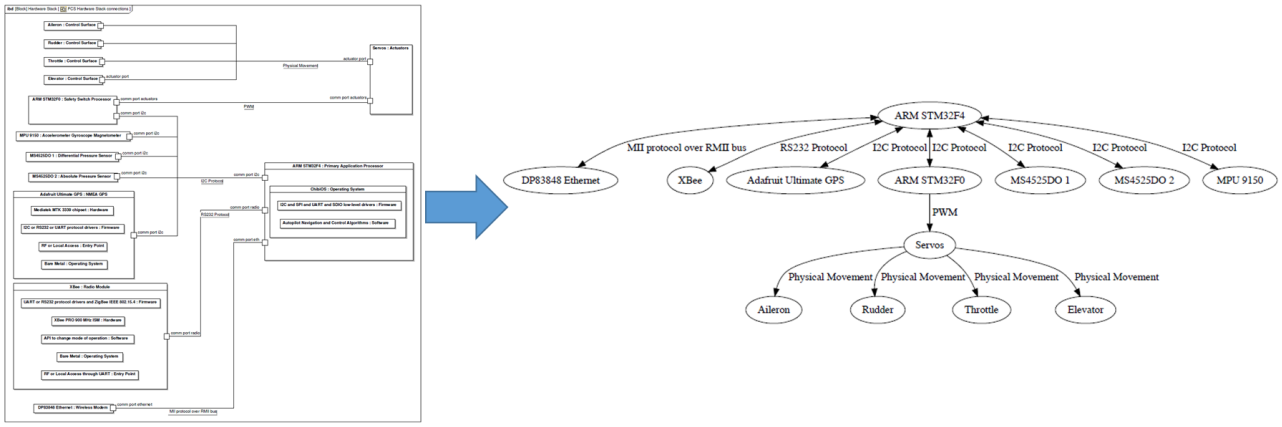


*Figure 7: SysML To Graph-Based Model (Bakirtzis et al. 2018)*

The goal of this resulting graph model of the system is to traverse known attack and vulnerability databases that are hierarchical and interconnected such as Common Attack Pattern Enumeration & Classification (CAPEC) – capec.mitre.org, Common Weakness Enumeration (CWE) - cwe.mitre.org and Common Vulnerabilities and Exposures (CVE) - cve.mitre.org. Using search tools such as CVE-SEARCH PROJECT, cve-search.org we can then automate using Natural Language Processing (NLP) the graph traversal paths to identify recorded attack vectors. We assume system vulnerability if any attack vector exists in the databases that map to the attributes of the system model.

Currently, system designers do not typically check for vulnerabilities for all their system components. If implemented, this process enables security by design. The disadvantage of this process is that it is incapable of detecting zero-day vulnerabilities never discovered, reported, and recorded before. However, this process still can work on a proprietary database of vulnerabilities to extend the scope from the publically available MITRE databases.

### *3. Dynamic System Model*

The last model we look at in this paper is the dynamic systems model that can test the robustness and resilience of the temporal behavior of the cyber-physical system. This technique is based on a control theoretic framework (Xue et al. 2012) as modeled by the state space equations below:

$$\frac{dx}{dt} = Ax + Bu$$
$$y = Cx + Du$$

These equations describe a continuous-time State-Space Model which is shown here as an example. We could also use a discrete-time model without loss of generality of the technique. The goal is to accurately model the temporal dynamics of any system be it continuous, discrete or hybrid. In the above equations, *x* is the state vector, *u* is the input vector, *y* is the output vector, A is State Matrix, B is Input Matrix, C is Output Matrix, and D feedthrough Matrix. We use control theoretic properties to study the system's vulnerabilities. For example, 'observability' is a measure of how knowledge of its external outputs can infer the internal states of a system. Observability and controllability of a controlled system are mathematical duals. These properties can be computed from the above system matrices.

Why is this model useful in evaluating cybersecurity? We can create an asymmetry between offense and defense. Our goal in cybersecurity defense is to create such a significant asymmetry, that offense is very expensive or of very low probability. Let us analyze this from an adversary's perspective. The adversary can be assumed not to have full knowledge of the system that they wish to attack. Their goal is to penetrate a subset of nodes, lay dormant and observe the behavior of these compromised nodes. Their next goal is to study Network Topology (Structure) and decipher the hidden Dynamics. The system designer intends to ensure that limited observation from minimally compromised nodes does not allow the attacker to get the network topology or dynamics. In short, if the observability of the network is low, then the attacker cannot attack the system quickly. Low observability then means that the controllability of the system also is tedious. There is a tradeoff as to where this balance is. Thus, when cybersecurity is an additional design criterion to system performance, the tradeoffs have to be rethought carefully.

In systems such as DP where the structure and dynamics are subject to complex stochastic environmental variations, the design introduces new challenges.

This framework can help us analyze and quantify security. We can develop metrics based on the difficulty of obtaining structure and dynamics info and use these to compare our design tradeoff options. We can also enhance our models from attack by taking non-commensurate sensor fusion (GNSS, Acoustic & Inertial) to a higher level of model fusion using these control-theoretic models.

## Principles to Secure Cyber Systems

In addition to the modeling techniques above, there are some general guidelines for securing cyber systems (MIT xPro Cyber). Proactive security measures include 1) Prevention and 2) Resilience under attack and reactive measures include 3) Recovery after the attack. Prevention tactics include a) Complete Mediation, b) Separation of Privileges, and c) Principle of Least Privilege.

Complete mediation says if we care about a property, enforce it every step of the way on every single instruction. If every access, every request by anybody on the computer system is checked, the system becomes safer. Otherwise, if we miss even one check then, of course, the attacker could exploit it. The general thought is that application programmers are thinking at a high level, so it is best if hardware or OS implements this strategy to improve efficiency. There is a computational cost to this strategy, and so hardware is computationally the best level to achieve complete mediation, but this puts a burden on flexibility for changes in design after implementation.

Separation of privileges is already implemented in DP subsystem modules using the seven pillars of DP design and security (Purser, 2013 & Cadet and Rinnan, 2016). If there is a security exploit in one module, it does not affect other modules. Even though there is a performance price to be paid for module separation, it might be well worth the effort, to ensure security. Separation is also not a guaranteed

foolproof methodology, as separate modules have to talk to one another to be useful. We want to make it harder for the malicious adversary to take advantage. The higher and stronger the fence the more secure we could be.

The principle of least privilege implies every user should be given no more than what is required of them to do their job. Classified information is handled similarly with a need to know. There are different tier levels for what we need to know. This compartmentalized separation of information and giving access to only those who need to know maintaining the principle of least privilege is how nations ensure that secrets are kept safe. This is a general principle of security, scalable across domains. This principle applies to physical assets also such as control room entry and permission to control assets.

Resilience under attack can be implemented using a) encryption or b) redundancy. Encryption helps prevent information leakage even if accessed by the intruder, as they are incapable of deciphering the content. Redundant systems on ships also support resilience. Redundant ship systems were designed to prevent catastrophic operational failures at sea. However, this idea of redundancy translates well to strengthen cyber systems. The goal is to provide guaranteed operation despite failures. Once the attack is detected, we can isolate the corrupted system and then switch to the redundant backup to continue. As with all systems, there is a cost penalty for supporting redundant systems. Hence, we need to determine which subsystems need to be duplicated, judiciously. This redundancy in critical subsystems provides fault tolerance, one of the seven pillars of DP design (Purser, 2013 & Cadet and Rinnan, 2016).

Reactive security measures use recovery after attack process 1) Detect 2) Isolate and 3) Recover. Using anti-virus software and restoring to a prior safe checkpoint state is common in IT systems. The general principle is to keep track of states and fall back to a safe, known state when the system is corrupted.

The use of general principles to secure systems increases asymmetry and make it difficult for the malicious actor to penetrate and corrupt the system.

## Future Possibilities

In this section, we discuss some of the latest technologies and issues that could affect cyberspace and its security.

### *Quantum Computation, Communication & Encryption*

Quantum computers work on particles that are in superposition thereby enabling parallel computations of a multitude of states simultaneously. If we can physically realize such a machine at scale, then modern day encryption will be cracked. Current systems using encryption as a means to ensure resilience under attack will be at risk. We hope that quantum cryptography will then come to our rescue assuming that it will scale to all systems that require encryption. However, there are arguments against quantum computers being able to scale (Moskvitch, 2018). Only time will tell.

Quantum communication implemented through quantum entanglement occurs when a pair of particles interact physically, even though separated by a distance. Einstein's famous "spooky action at a distance" property of entangled quantum particles can be separated by large distances of the order of hundreds of miles or even more. Recently the Chinese have demonstrated the transfer of information across 1200 kilometers thereby providing the technology for ultra-secure communication networks and, eventually, a space-based quantum internet (Popkin, 2017). This technology will help prevent signal spoofing, but signal jamming and denial of service might not be avoided.

### *Multiparty Computation*

Fully homomorphic encryption is a technology that can carry out arbitrary computation on encrypted data. This technology when mature will prevent many of the data breaches that have been in the news lately. All data will be encrypted and hence remain anonymous. Unfortunately, fully homomorphic encryption has a computational load that is close to multiple orders of magnitude compared to computing on unencrypted data and this technology is not yet ready for prime time. When available, this technology will be a case of resilience under attack. Partial homomorphic encryption where some limited functions can be implemented on distributed encrypted data with reasonable computational load could help transition as the technology matures. By keeping the data distributed and encrypted across multiple subsystems or nodes we not only apply the principle of resilience under attack due to encryption and redundancy we can also add another layer of protection due to the separation of privileges. Combining different principle of protection increases asymmetry and hence burden on the malicious user to penetrate such systems.

### *Artificial Intelligence (AI) & Machine Learning (ML)*

Currently, there have been advances in Artificial Intelligence (AI) and Machine Learning where zero-day attacks, attacks never seen before can be detected. These generally use the technique of anomaly detection changes in typical patterns of behaviors to look for potential attack vectors. Anomaly detection uses baseline operations to flag, unusual behavior from the normal.

Behavioral analytics is a new cop in town. Earlier this year Palo Alto Networks introduced Magnifier, a behavioral analytics solution (Oltsik, 2018). Generally, a man-machine symbiosis approach works best where ML algorithms flag unusual behavior and the human in the loop can verify if new behaviors need to be blocked.

The major impediment to these technologies scaling is privacy and sharing of data across companies. We can get around these privacy issues using homomorphic encryption, and then defensive techniques will not be so fragmented and will have higher success.

### *Blockchain*

A blockchain is a decentralized, distributed; public digital ledger used to record transactions so that the list of records called blocks cannot be altered retroactively without alteration of all subsequent blocks. The blocks are linked and secured using cryptography. Blockchain technologies were developed through breakthroughs in cryptography and security. It offers a secure approach to storing information, making transactions, and establishing trust with mutually unknown actors. We will need to watch out for quantum computations that could make current encryption technologies defunct.

Here are some examples that use blockchain to enhance cyberspace security. Guardtime used blockchains to create a Keyless Signature Infrastructure (KSI) and secured all of Estonia's 1 million health records with its technology (Guardtime, 2007). REMME’s blockchain can authenticate users and devices without the need for a password (REMME, 2016). Recently collaborative effort between the world’s largest shipping company, Maersk, and IBM has now grown to 92 participants to help implement supply chain record keeping using blockchains thereby enabling distributed information sharing (Castillo, 2018).

### *Ethics*

Cyberethics is the philosophic study of ethics about computers and the users who use them. The critical goal is to study how user behavior on computer networks affects individuals and society. The ten commandments of computer ethics state that though shall not interfere, harm, steal, snoop on others

property (Barquin, 1992). It also says that we should think about the social consequences of the systems we are designing. A discussion on ethics leads us to cyberwarfare and autonomous weapons driven by AI. We should have open debates about these topics as a society and put policies in place to ensure we do not self-destruct. Unlike mutual nuclear deterrence using the principle of mutually assured destruction (MAD), cyber warfare is a little fuzzy given that non-state actors can have access to this technology and without a geographic boundary to contain the adversary, it becomes challenging to defend against these threats. We hope law and policy on these issues will catch up to the speed of newer technologies.

## Conclusion

In this paper, we show that DP systems are Cyber-Physical Systems (CPS) that due to interconnection with numerous other complex systems behaves as Complex Adaptive Systems (CAS). We then proceed to discuss cybersecurity from a systems perspective arguing why security, a negative goal, is challenging to prove. We then show that DP systems are a fusion of information technology systems and operational technology systems, known as cyber-physical systems.

We argue that the lack of trust in information propagation is the key to a lack of robust security. We also opine that since humans control some cyber systems, these nodes of the network could have malicious activity as present in society. Creating an asymmetry for the malicious actor is one way to prevent penetration into the system and hence resulting attacks.

The attempt to model such CPS systems at different levels of resolution enables us to study the security properties of such systems more in-depth and generate metrics that can help us quantify the risk to potential vulnerabilities. Enhancing sensor-based fusion to model-based fusion increases our security posture. We then show how such models could improve security by design. We also advocate for using standard principles to secure such systems. This combination will increase asymmetry for the malicious actor and make it difficult to penetrate and corrupt the system.

We conclude by introducing some future technologies that might alter the cybersecurity landscape for cyber-physical systems such as dynamic positioning systems.

## References

Bakirtzis, G., et al. (2018) “A Model-Based Approach to Security Analysis for Cyber-Physical Systems,” arXiv:1710.11442v3 [cs.CR] 10 June 2018

Barquin, Ramon C. (1992), "In Pursuit of a 'Ten Commandments' for Computer Ethics," http://computerethicsinstitute.org/publications/tencommandments.html, Computer Ethics Institute, retrieved Sept 15, 2018.

Biber, Daniel (2018) “Bundles of birds in the sky figurine created a giant bird,” https://telegrafi.com/tufa-e-shpezeve-krijuan-ne-qiell-figurene-nje-zogu-gjigant-foto/, retrieved Sep 15, 2018.

Guardtime, (2007) "KSI Technology Stack" https://guardtime.com/, retrieved Sept 15, 2018.

MacDonald, James (2017) “How Do Fish Schools Work?” https://daily.jstor.org/how-do-fish-schools-work/, June 21, 2017, retrieved Sep 15, 2018.

Michael del Castillo (2018) “IBM-Maersk Blockchain Platform Adds 92 Clients As Part Of Global Launch”, https://www.forbes.com/sites/michaeldelcastillo/2018/08/09/ibm-maersk-blockchain-platform-adds-92-clients-as-part-of-global-launch-1/#6851009468a4, Aug 9, 2018, retrieved Sept 15, 2018.

Miller, John H., and Scott E. Page (2007). "Complex adaptive systems: an introduction to computational models of social life," Princeton University Press. ISBN 9781400835522. OCLC 760073369.

MIT xPro Cyber, MIT Professional Education's Cybersecurity course - Cybersecurity: Technology, Application and Policy https://mitxpro.mit.edu/courses/course-v1:MITProfessionalX+CSx+2016_T2/about, retrieved July 30, 2018.

Moskvitch, Katia (2018), "The Argument Against Quantum Computers" February 7, 2018, https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/, retrieved Sept 15, 2018.

Olivier Cadet & Arne Rinnan (2016) "Who Said That DP Does Not Rhyme with Cybersecurity?" cybersecurity session, DP Conference, Oct 11-12, 2016, Houston, Texas.

Oltsik, Jon (2018), "Artificial intelligence and cybersecurity: The real deal," CYBERSECURITY SNIPPETS, Jan 25, 2018, https://www.csoonline.com/article/3250850/security/artificial-intelligence-and-cybersecurity-the-real-deal.html, retrieved Sept 15, 2018.

Patrick Honner (2018), "How Math (and Vaccines) Keep You Safe From the Flu" https://www.quantamagazine.org/flu-vaccines-and-the-math-of-herd-immunity-20180205/ Feb 5, 2018, retrieved Sept 15, 2018.

Popkin, Gabriel (2017), "China's quantum satellite achieves 'spooky action' at record distance" http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance, Jun. 15, 2017, retrieved Sept 15, 2018.

REMME (2016) "The time has come to finally secure your business" https://remme.io/, retrieved Sept 15, 2018.

Richard Purser (2013) "Meaning of LIFE," Quality Assurance Session, DP Conference, Oct 15-16, 2013, Houston, Texas.

Stonedahl, F. and Wilensky, U. (2008), " NetLogo Virus on a Network model," http://ccl.northwestern.edu/netlogo/models/VirusonaNetwork. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.

Xue, Mengran; Roy, Sandip; Wan, Yan and Das, Sajal K., (2012) "Security and Vulnerability of Cyber-Physical Infrastructure Networks: A Control-Theoretic Approach" in "Handbook on Securing Cyber-Physical Critical Infrastructure" edited by Das, Sajal K., Krishna Kant and Nan Zhang, Morgan Kaufmann, Elsevier, MA USA. ISBN 978-0-12-415815-3