OMNIA Cybersecurity Architecture

An Inclusive Governance Model

for Self-Sovereign Cyberspaces

Authors: Ben Koo, Sue Kamal

OUTLINE

Executive Summary

The omnipresent communication and computational activities in physical spaces have awakened a new kind of security awareness. Given the unprecedented speed and scope of data processing capabilities brought to us by wirelessly connected mobile devices, tiny organizations could operate data intensive global operations and deploy digital content to millions with near-zero barriers to entry. These emerging cyberspace capabilities disrupt the existing social orders, and even influence global and regional politics through AI-enhanced social media wars. While more advanced cybernetic infrastructures will accelerate data distribution, content creation, and supply chain orchestration, the accelerated activities also introduce unprecedented vulnerability in existing political, economical, and cultural systems. Systematically identifying, classifying, and controlling societal vulnerability induced by the forever changing cybernetic infrastructures is the grand challenge that threatens the destruction of human species, now.

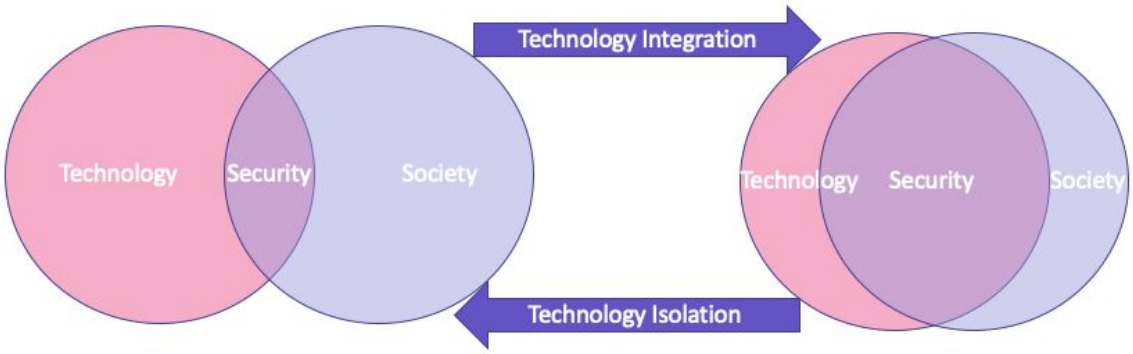
To tackle cybersecurity challenges at its root, Omnia Cybersecurity Architecture (OCA) presents an inclusive cyberspace governance model that is designed to ***continuously utilizes the most up-to-date solutions***. Using the case of high-frequency trades as a concrete example, “Those who have the fastest network connections win”. By attaining comparatively higher-speed network connections, market hackers can break information symmetry and therefore repeatedly induce violent fluctuations in global marketplaces. This symmetry-breaking principle in cyberattack orchestration applies to a broad range of malicious and unintentional acts. Intentional actions include Denial-of-Service attacks designed to shut-down critical public infrastructures, social media hacking, designed to use computer-controlled media wars to alter political outcomes. These seemingly disconnected cybersecurity scenarios all share the same root: ***the speedy exploitation of information asymmetry***. A sound security approach should embed this symmetry-breaking detection pattern to prevent and deter security-breach scenarios at its core. Henceforth, OCA guides people, processes, and technologies to enable organizational awareness of abnormal asymmetries in a timely manner. OCA also aims at the broadest possible participation. It openly invites either individuals or government agencies to utilize its design principles, and contribute to its security policy repository as a creative common. OCA distinguishes itself from existing security architectures that have inherent commercial and political interests by maintaining transparency and inclusivity. Organized as an open security standard consortium, OCA welcomes cybersecurity experts, government representatives, enterprise leaders, and technology standard definition societies, to join force in the creation and refinement of a ***symmetry-preserving cybersecurity architecture***.

Prologue:
Emergence of the OMNIA Cybersecurity Architecture

As the technologies encroach into the inner fabric of human activities, a different kind of security awareness is emerging. As Winston Churchill once said:

"We shape our houses, thereafter they shape us!"

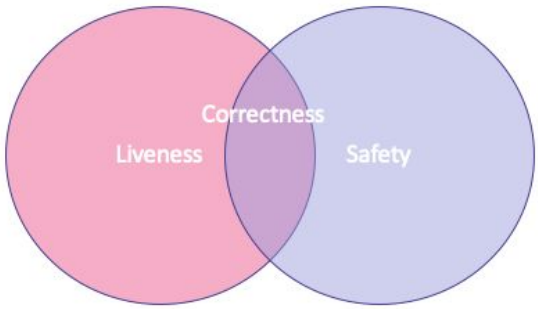
At time of this writing, a reliable, yet nimbly adaptive cybersecurity architecture is still being shaped by the best and brightest minds. However, so far, a dominant solution has yet appeared in our daily use of cyberspace technologies. To visualize the nature of this immense challenge, we can see how cybersecurity experts, Bell, et. al.[1] look at the contentious forces in the field of cybersecurity practice:



Modified from Figure 1-1 and 1-2 of Agile Application Security: Enabling Security in a Continuous Deliver Pipeline, by Laura Bell, Michael Brunton-Spall, Rich Smith & Jim Bird, O'Reilly Media, 2017

The challenging nature of cybersecurity is embedded in the interlocking structure of cybernetic connections. When one introduces more technological remedies to create an integrated solution, the more areas of security concerns must be protected, causing an infinite cycle of coupling and decoupling. The iterative refinement nature of cybersecurity practice appears to be an inescapable reality. We don't seem to have a choice, since Global Connectivity is not driven by one singular force, there are many parties at work to introduce

all types of cybernetic interconnections. From a technologist's viewpoint, the world seems to be moving toward a more integrated whole, and we just need a different way to look at this entangled problem.



The Theoretical Definition of System Correctness

The above diagram is an architectural viewpoint of designing a pragmatic cybernetic system. A "***correct***" system is one which simultaneously fulfills both safety and liveness conditions. The intersecting area in the venn diagram, is the ***correct*** functional area that engineers strive to operate within. As defined in Koo's doctoral thesis[2],

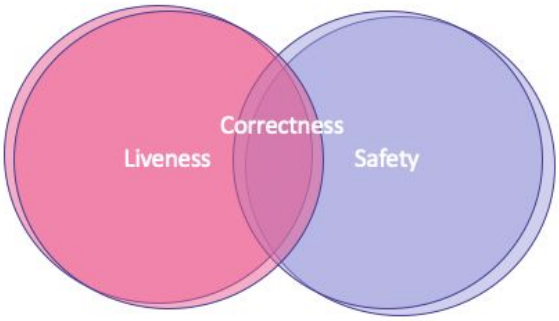
> ***"A system's architecture simply denotes the stable properties of a system."***

This engineering approach is not about making choices between the balancing acts of integration and isolation. It is about identifying the overlapping functional areas that the same, unchanging system may continuously deliver both safety and liveness at all times. As Turing Award Winner, Leslie Lamport defined in one of his seminal papers: Proving Liveness Property in Concurrent Systems [3]:

> ***Safety:*** Something bad never happens
>
> ***Liveness:*** Something good eventually does happens

Without immediately jumping into the clever mathematical techniques that Lamport used to reason about complex system correctness, it is the view angle that seeing the overall cybernetic system as a single system, being continuously, and incrementally modified to

provide the “eventual” good things that provides a “correct” path to develop and operate a cybersecurity system.



The Inremental Change Approach promoted by DevOps/CICD practitioners

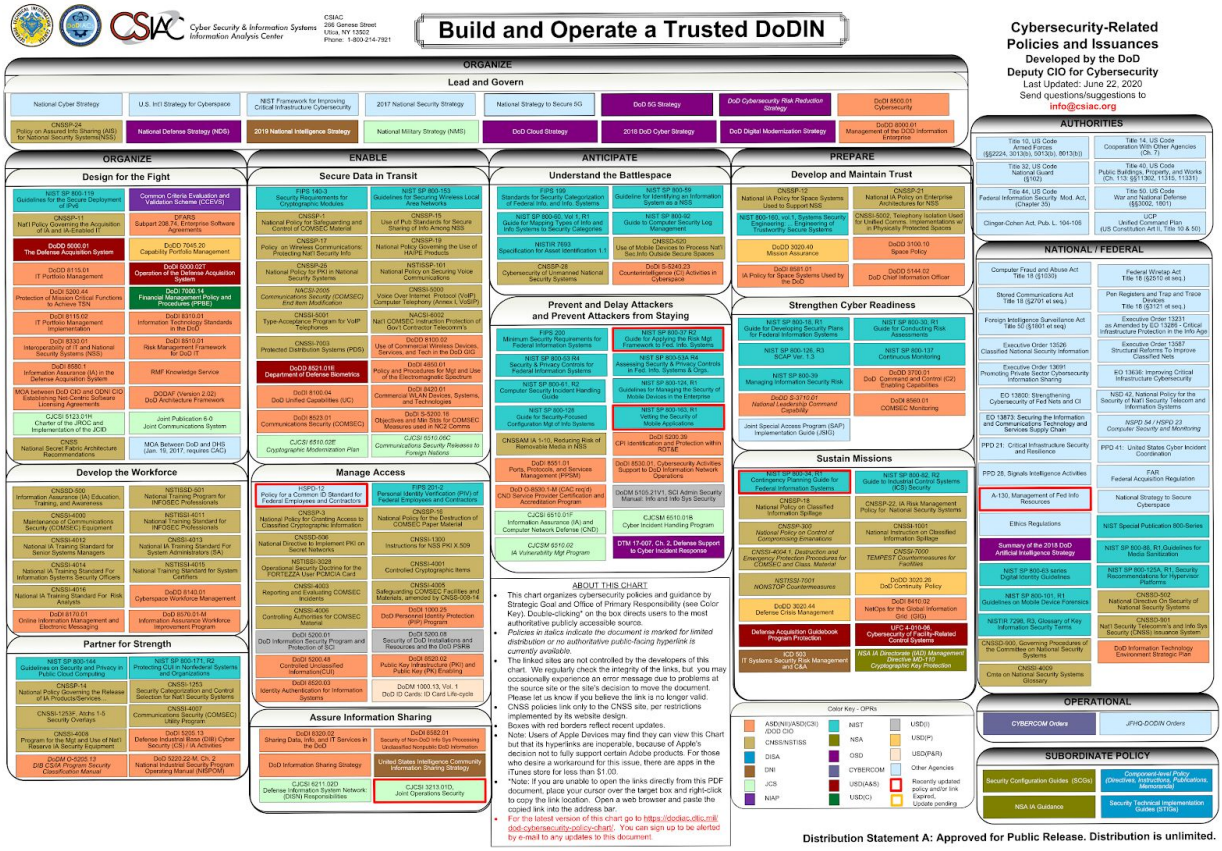
In fact, this incremental approach what DevOps[1]/CICD[2] proponents are already doing in the field of Information Communication Technologies(ICT). So far, DevOps/CICD has proven to have expedited the speed of technology integration in many industries, from telecommunication, software development, to manufacturing and supply chain management[4]. However, the focus of DevOps/CICD is to accelerate technology infusion, and these accelerated practices may not be compliant with societal or governmental security regulations. In certain cases, the aggressive technology infusion schedule in the social media industry can be particularly suspicious. Therefore, an improved version of DevOps/CICD, called ***DevSecOps***[3] has been introduced, to ensure that security verification and compliance checks are incorporated at all stages of development/operational activities.

DevSecOps is a hot topic in ICT-intensive industries, but it is not yet a turn-key solution that casual users could start practicing it at home. To practice DevSecOps adequately, it usually requires a team of competent ICT experts, each knowing a few areas of the inner workings of ICT toolchain. On top of that, these experts need a very good management system to coordinate their efforts. In other words, most enterprises or small organizations simply

[1] DevOps stands for Development and Operations of ICT systems.
[2] CICD stands for Continous Integration and Continuous Deliver/Deployment
[3] DevSecOps stands for Development, Security, Operations.

cannot afford to find and hire these elite experts. DevSecOps can be difficult and expensive. Many forward thinking organizations are searching for either a low barrier-to-entry solution, or a solution that could deliver cybersecurity solutions at scale, ideally, both low barrier-to-entry and scalable.

June 22, 2020, the Cyber Security & Information Systems Information Analysis Center of the Department of Defense of US, recently created a document titled:"Build and Operate a Trusted DoDIn". It was intentionally designed and ***authorized for unlimited public distribution***. This document covered a wide range of functional areas and agencies within the US government, including the White House's vision of its National Cyber Strategy. The document is a matrix-like diagram, each cell can be clicked-on and linked to another document. It is a good reference to see how the United States Government plans to protect and serve its people and keep "Prosperity, Security and Openness in a Networked World". The last phrase is a subtitle of one of the indexed documents titled: International Strategy for Cyberspace. All these documents can be directly found on the visual layout of this chart is shown below:



This chart[4] covers a wide range of Cybersecurity Policy concerns that is truly overwhelming. On the webpage that publicizes this document, the first sentence says:

"The goal of the DoD Cybersecurity Policy Chart is to capture the tremendous breadth of applicable policies, some of which many cybersecurity professionals may not even be aware, in a helpful organizational scheme."

If some hackers decide to challenge the Cybersecurity Supremacy of the USA by reading this document, the "tremendous breadth of applicable policies" of this chart would definitely have achieved its goal of deterring such hackers. Clearly, no one person could finish reading that large collection of evolving documents, not even the Department of Defense agency itself. The possible inconsistencies amongst these myriad documents could already create security risks that are embedded in the governance model of cybersecurity policies. There should be a more intuitive way to articulate the cybersecurity protection principle of large scale socio-technical systems. Maybe it can be something very intuitive and simple.

The Principle of Information Symmetry

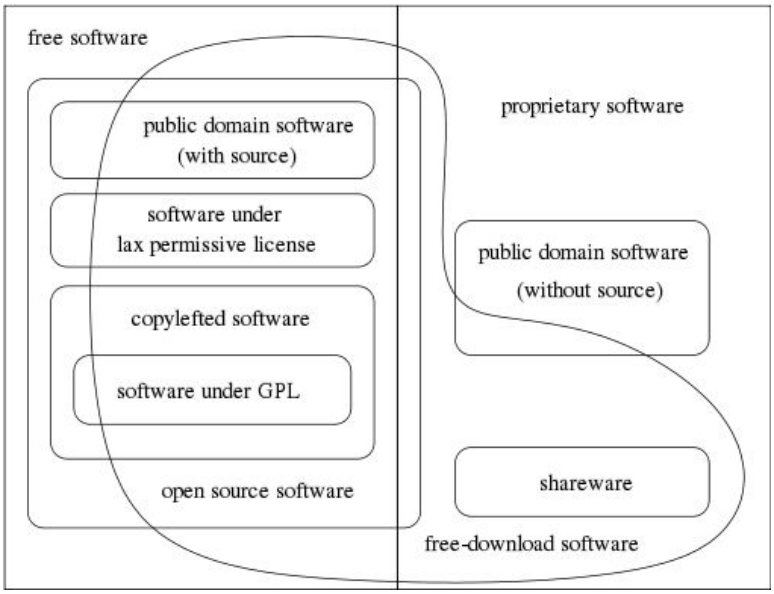
Maybe, cybersecurity policies shouldn't separate a networked society into hierarchical social classes of highly-connected citizens and those who are not-so connected. It should adopt an inclusive principle that covers the entire cybernetically connected world as one incremental adaptive system. For most citizens and nations, they are just trying to identify an area that they can operate in the "correct" zone, the zone where they can live safely, and they can create something good to demonstrate their liveness. Recall Turing Award Winner: Leslie Lamport, who formally defined Liveness and Safety, he also worked with Robert Shostak and Marshall Pease to use simple terms and analogies that are traceable by non-mathematicians to proof the technical case of consensus, often known as the Byzantine Generals' Problem [5]. Lamport also used diagrammatic techniques to illustrate the nature of Time, Clocks and Ordering of Events in a Distributed System[6]. It is the simplicity and elegance of these ideas that "eventually" gave us the roadmap to implement

[4] For the latest version of this chart, please go to https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

Bitcoin, Blockchain, and Crypto-Economic Systems. Therefore, it would be meaningful to think again about what and how can we pick a grounding thesis, so that our ongoing evolutionary efforts would lead us onto a journey that contains sufficiently abundant "correct" zones that simultaneously satisfies liveness and safety conditions?

Our answer is to offer an inclusive governance model for cybersecurity. First, we welcome everyone and any organization to participate in the creation and evolution of this document. Secondly, this document will draw on existing ICT cybersecurity practices, such as DevOps, CICD, DevSecOps, Service Mesh, container technologies, and other known work in the field of cybersecurity. These existing tools and methodologies will give us the vocabulary to articulate the scientific and technical concepts that paved our current understanding of the cyber-physical space in its current form. The third element is the toolchain that we are building to support the creation and evolution of a cybersecurity solution that adheres to the Principle of Information Symmetry.

It is necessary for cyberspace participants to know the classification of software license categories. The document is referenced here, and the diagram that illustrates the categorization is shown below: (Diagram created by Chao-Kuei, a link to its Scalable Vector Graph version is here.)



Picking the word, "copyleft" in mirror symmetry to the legal term "copyright" is not just a word game. GNU Foundation explained in the document: "What is Copyleft"[7], how to

leverage the balancing legal logic of copyleft to keep incentives for contributors to develop copylefted software in a world that protects copyrights. In the original words:

"To copyleft a program, we first state that it is copyrighted; then we add distribution terms, which are a legal instrument that gives everyone the rights to use, modify, and redistribute the program's code, or any program derived from it, but only if the distribution terms are unchanged. Thus, the code and the freedoms become legally inseparable."

GNU's copyleft legal framework effectively transformed the way our cyberspace is being operated and regulated. It was the "legally inseparable" distribution terms that converted a very significant portion of software to be copylefted. Copyleft continuously draws many active developers to write code under copyleft terms, it also shapes the developmental dynamics of commercial and free software products. ***This demonstrates that copyleft is a practical governance model.*** Copyleft as a legal device, provides an important clue for maintaining the balance of liveness and safety in a collective cyberspace as large as the Internet. The following phrases, left vs. right, architectural properties, invariance, balancing acts, logical consistency, equivalence, sustainability and consistency, can all be associated with one mathematical idea: the notion of symmetry. It is the Principle of Information Symmetry that readers of this document should keep in mind. It is based on the symmetry-checking viewpoint, that we invite all of you, who read this document, to help develop the conceptual frameworks, the architectural compositions, and the technological solutions, and present counter-balancing challenges that will make this document a living document that "eventually" be useful and safe-enough for the development and operation of cybersecurity systems. When and wherever possible, we encourage all participants to follow the copy-left licensing agreement as defined by Free Software Foundation:

"Free software" means software that respects users' freedom and community. Roughly, it means that the users have the freedom to run, copy, distribute, study, change and improve the software.

Ben Koo, Sue Kamal

July 14, 2020

Bali, Indonesia

Context: Contemporary Cybersecurity Threats

The year 2020 is a good year to embrace hindsight. A good part of this year, the whole world was put under intermittent movement restrictions caused by Covid-19. The isolation of physical contacts elevated the functions of Information and Communication Technologies (ICT) from its supportive roles in the past into the current leading role. Without the ubiquitous ICT penetration, the outcomes of global outcomes may be much worse, because more chaos will be created by information asymmetry due to movement restrictions. As more people rely on ICT tools, cybersecurity becomes a more pressing concern. There could be more users who just recently begin to rely on ICT for their livelihood, and they can be exposed to a lot more risks than they ever imagined. Information leaks, identity theft, fake news, to name a few, any of these seemingly benign terms can be lethal, but most people have not learned to cope with these new dangers, now their lives are already dependendent on ICT infrastructures.

Technologies can be either good or bad for society, but the uneven distribution of technical capabilities will cause problems for sure. One may argue that information asymmetry about the epidemic nature of Covid-19 was a major cause of this unprecedented global disaster. This incident unveiled a new paradigm of warfare strategy: information asymmetry can be weaponized to inflict damages at a very large scale. Unfortunately, our collective cyberspace is also being threatened by dark forces incommensurable to most people. Asymmetric utilization of social media technologies in political campaigns[5] have influenced strategic political outcomes in several nations. By now, it is generally recognized that new ICT capabilities can induce unfair advantages in political campaigns, economic development programs, and can shift cultural norms. With the incoming wave of 5G deployment, many more industries and social practices will be transformed by the massively expanded mobile data bandwidth and lower network latency. These communication infrastructure enhancements will enable new, expanded ICT capabilities ranging from personalized social media applications, crypto-currencies, design automation,

[5] According to Wikipedia, the political consulting firm, Cambridge Analytica Ltd, combined data analysis with proactive communication techniques to influence electoral processes in multiple nations.

autonomous vehicles and machine learning algorithms. Each one of these new ICT-enabled capabilities has the potential to trigger a major surge in industrial productivity and market exchange efficiency. As socio-norms and business operations equip themselves with these new ICT-enabled capabilities, freely available open sourced technologies licensed under the Free Software copy-left agreements, will also fundamentally shift the paradigm of economic distribution and societal governance. The global society is collectively facing the challenge to search for a sustainable governance model in cyberspace that can handle the combined effects of these new and emerging ICT capabilities. To cope with these emerging challenges and unforeseen compound impacts of ICT, a concise, yet operational framework, that can tackle these threats is sorely needed. This document introduces Omnia Cybersecurity Architecture (OCA) as an ***inclusive governance model*** to diagnose and tackle existing and emerging threats with one unifying security protection principle: sustain system safety and liveness via the maintenance of information symmetry.

Goal: Governing Cybersecurity based on the Principle of Information Symmetry

The goal of this document is to present a generally applicable model of cybersecurity governance, so that human lives and human's basic needs can be protected. In order to operate a sustainable socio-technological infrastructure, universal accessibility to ICT is a new fundamental requirement for modern human civilization. As new technologies continuously being integrated through the global ICT network, our world is becoming a cyber-physical space, a physical space that is heavily monitored and controlled by ICT. Maybe some literature still consider cyberspace and physical spaces as two separate domains. With the ubiquitous deployment of Internet of Things (a.k.a. IoT) technologies that embed programmatically controlled networked sensors and actuators into physical spaces, cyber-physical spaces and cyberspaces are practically indistinguishable. In this document, we will use the two terms, cyberspace and cyber-physical space, interchangeably[6]. This integrated view of cyber-physical systems is not a rhetorical one, it has direct causal consequences regarding the integrity of overall system security. The security breach in either physical space or cyberspace, will eventually compromise security in the other. Given the dominating social impact of ICT, many national governments have recognized the need to regulate activities in cyberspaces. However, the dynamic and technical nature of ICT, which defines the operational properties of cyberspaces, continuously challenges the practical interpretation of laws, and therefore changes the way laws can be enforced. According to constitutional law scholar, Lawrence Lessig[8], the regulatory process that makes new laws and the law enforcement[7] activities, must be continuously updated to leverage the capabilities offered by late-breaking ICT. Given the premise that private properties and data assets are protected, to maintain order and justice in cyberspace, all stakeholders must have symmetric access to not only public information[8], but also the accompanying technology development methodology. Operationally, the awareness of public goods must be embedded in the developmental

[6] The term: "physical space", simply means physical space. It is not interchangeable with cyberspace.
[7] This idea was derived from Constitutional Law scholar, Lawrence Lessig. His 1999 book Code and other Laws in Cyberspace spelled out this explicitly.
[8] The notion of "private ownership" by definition, should allow all parties to enjoy their privately owned data and intellectual properties just to themselves, unless they willingly decide to share them.

process of new technologies. In practice, policy makers and policy making procedures should adopt ICT empowered tools and methods, so that policy compliance and public interests can be an integral part of the technology developmental process. In short, the goal is to attain information symmetry at all times. In practice, we propose the following solution:

Create a *reference model* for *cybersecurity governance* that enables cybersecurity compliance across all stages of critical public infrastructure development and operational activities, using the most inclusive infrastructure, data formats, and human interfaces to ensure *sustainable egalitarian access.*

The reference model mentioned above, will consist of the following components:

1. A set of conditions: These conditions are mandated rules that examine the compliance to the proposed inclusive governance principles.
2. A set of governance model outcomes: the outcome consists of the basic requirements of a cybersecurity agency, the functional requirements of its cybersecurity integrated reports, reporting mechanisms, and supporting tools that enable the ongoing cybersecurity policy governance.
3. A meta-governing process: This is a generalized process model that explains the mechanism of governance. How and why it needs certain elements to enable self-sovereign governance to be practiced within an organization.
4. The necessary resources and building blocks to enable the process model.
5. The boundary conditions that may break the assumptions of the above mentioned governance model.

It is important to note that a reference model only prescribes the architectural, or the stable, unchanging elements of a real-world operation. The working detail of cybersecurity operations is not covered within this document. This document is not an operational manual to create and implement all the cybersecurity infrastructures. It only provides a principled guideline to conduct governance activities in shaping and changing cybersecurity policies. This document also presents what basic technical elements are required to label or name the resources that must be protected. The document also includes references to existing organizations and technology suppliers that offer solutions compatible to the guiding principle of this document.

Cybersecurity Compliance through Measurable Effects: Correctness = Safety + Liveness

An operational framework that can orchestrate people, process, and tools to maintain the overall correctness condition can be prescribed in a technical implementation architecture. This document presents Omnia Cybersecurity Architecture (OCA) to explicitly define the conditions to operationalize the governing principle: maintaining information symmetry. Paraphrasing the definition of technical architecture based on ISO/IEC/IEEE 42010[9]:

To be OCA-compliant, technical systems must abide by the following five conditions to organize stakeholders, processes, and technologies that enable the design and evolution of cybersecurity governance.

The objectives of ensuring information symmetry can be verified in the following ways:

1. Embed cybersecurity compliance verification procedures into product/service development and operation management activities using programming interfaces that enable transparent access to qualified security administration. These programming interfaces will be published as OCA-compliant Programming Interface Standard (OCA-IS).
2. For products and services related to public safety, all technology suppliers involved in the development or operational aspects of the system are required to continuously publish safety compliance verification data to the public via the OCA-IS.
3. Operational history data that should be exposed to the public as a medium for trust-worthiness evaluation must be recorded and maintained using immutable data infrastructures. OCA-compliant data log (historical data, OCA-DL) that represents public cyberspace activities in real time, should be recorded using an openly accessible immutable database. This data log and every data entry's order of appearance can be witnessed by the public, therefore hold relevant participants accountable for their time-stamped activities in public[10] spaces.
4. Data content in OCA-DL should be presentable in popularly accessible browser software and mobile computing devices, so that the data could be conveniently

[9] Please refer to the official website on ISO/IEC/IEEE 42010 on its website: http://www.iso-architecture.org/42010/.
[10] It is important to note that operational data in private cyberspaces should not be publicized.

viewed and analyzed using data visualization and data mining techniques at large. So that OCA-DL can be processed and analyzed using any data processing tools based on interoperable protocols. OCA-DL's information access right is protected by OCA-IS.

5. Dedicate developmental resources to create OCA-compliant educational material (OCA-EM) for all OCA-compliant Cybersecurity Technology development projects. The mandate in securing investments in OCA-compliant educational content development is to ensure the principle of information symmetry. This OCA-EM can also enable other industries and interested parties to learn from past projects and apply the principle of information symmetry to protect and serve their own interests while minimizing conflicts against others.

The above-mentioned five interrelated OCA-compliance requirements are all mandatory conditions to establish a robust architecture for cybersecurity. Only by adhering to all these conditions at all times, a global scale cybersecurity system can be guided and organized by a consistent and sustainable system governance principle: the Principle of Information Symmetry. This principle presents a disciplined approach to manifest trust and system integrity in the long term. Without operationalizing information symmetry into the developmental process of hardware and software products, cybersecurity-sensitive technologies would always have undisclosed backdoors that can be conveniently hidden in the developmental work. By promoting information symmetry, the chance of hiding or injecting loopholes can be systematically diminished. Trust-worthiness of relevant cyberspace systems can be compared and examined based on openly shared developmental process data and non-proprietary operational data.

Expected OCA-Process Implementation Outcomes

To implement a sustainable cybersecurity practice requires a number of preparatory actions and technological instrumentations. The requirements would naturally vary across different organizations, since each organization has different practical needs and also allocates different resources dedicated to preserving their desirable level of cyberspace safety. To operate self-sovereign cybersecurity in practice, the operating organization must fulfill a minimal set of resource requirements. These resource requirements are the outcomes of the OCA-compliance implementation process. OCA defines these implementation outcomes as follows:

Implementation Outcomes:

1. ***An adaptive Cybersecurity Governance Agency***: A cybersecurity administration agency should be established and be responsible for defining the classification rules of public and private data assets. When a data access/submission action is posted, a proper and equitable content release mechanism can work under the data administration framework. This agency will be tasked to implement effective data security governance through an automatic security policy execution system that utilizes a trust-worthy[11] resource identification namespace to keep all users accountable for their data access/submission actions. Based on OCA-compliant policies, organization-wide security governance should be executed through a self-sovereign[12], realtime policy execution service that triggers adjustment to modify access rights of the system when security-threatening scenarios arise. This continuously adjusted security management service will create an enforceable authority in cyberspace. This data-driven security-enforcement mechanism can be used to infer causal relations and compute correlations across the boundaries of all interacting cyberspaces, providing referential data content to analyze and detect the pulse of impending security threats. The agency should also have the authority and the technical capability to issue and modify the operational procedures of the above-mentioned data asset governance machinery.

[11] Trust-worthiness is achieved through technical means, as specified in OCA-compliance documents.
[12] Self-Sovereignty belongs to the organization that sponsors the cybersecurity administration agency.

2. ***An Integrated Reporting Framework for System Security***: The above-mentioned agency should have a single, unified, Integrated Reporting Framework[9] to reflect the real-time status of critical assets under cybersecurity protection. The agency must own and operate an extensible, yet integrative security status reporting framework as an essential instrument to enable proper organizational cybersecurity awareness. This reporting framework should be based on a machine-processable language to represent and execute the structural and quantitative policy concerns of cybersecurity. This language could utilize and extend on similar best-practices currently adopted by the ICT industry, such as OASIS's Security Assertion Markup Language (SAML)[10]. The adoption of SAML related data structures and machine-processable algorithms should be strictly compatible with OCA-IS as mentioned earlier. It will also be integrated with a dynamic user interface and data publishing framework to present cybersecurity concerns to relevant participants. To qualify the cybersecurity reporting framework as an integrative one, the design of the human-machine interface design must be sensibly embedded into the normal usage patterns of everyday workflow, meaning that all security-related information must be bi-directionally delivered in a consistent interface style on all relevant working devices, so that messages can be displayed in a unified and authoritative format. The controlling mechanism for defining the human-machine interface also needs to be compliant to OCA-IS, and it can be called OCA-HMI. An integrative reporting framework should provide universal accessibility, so that the security-related message could reach the broadest possible recipients on the most convenient devices, such as their personal cell phones or laptops. Being integrative also means that the cybersecurity reporting framework must be mindful of the cognitive load of its users. The informed users should only receive intuitive, timely, but not overwhelmingly frequent bombardment of alert signals. This framework will follow design ideas originally defined in the International Integrated Report Movement (<IR>), to provide a consistent, yet comprehensive measuring metric of the overall health condition of an organization that operates in cyberspace.
3. ***A Security-Aware Observability and Monitoring Infrastructure***: The above-mentioned Integrated Reporting Framework will be presenting security-related data content that enables organization-wide security status observability, elevates overall system security awareness through embedding

technical means to monitor data access, data submission, collection, extraction, transformation, loading, and delivery. Best practices in data visualization will be integrated with the cybersecurity observability and monitoring capabilities, so that proper system-level security awareness can be elevated using effective human-machine interfaces that are compliant to OCA-HMI. This observability and monitoring infrastructure is encoded with the OCA-IS programming mechanism mentioned earlier. The OCA-compliant agency should provide its data content through OCA-DL, and automate the security compliance verification machineries, through OCA-IS. All of the data presentation should be compliant to OCA-HMI, so that many of the cybersecurity verification procedures can be scaled up to serve the general public or the organization's intended user base.

4. ***A Trust-worthy Namespace Management System***: All data content, and data assets, must be organized in a consistent namespace (NS) management platform, namely OCA-NS, to be administered by the agency responsible for cybersecurity. Cyberspace accountability must be achieved through a unified, yet secure and privacy respecting resource identification (namespace management) system[13]. Globally applicable namespace management systems have been achieved through the Internet Protocol (IP) address, and Domain Name Service (a.k.a. DNS, the technical foundation of website and E-mail address management). However, as new communication technologies emerge, the concepts of Web 3.0, Spatial Web, Blockchain-based Timestamping Public Service, and Self-Sovereign Identification (SSI) technologies are some namespace management services that will have major implications in the arena of cybersecurity. As OCA-compliant cybersecurity policy is implemented on an organizational level, operational data must be referenced through a universally acceptable space, time, and identity namespace. The term, universal, refers to the "Universal" Resource Identification/Locator (URI/URL) scheme, originally introduced through the World Wide Web Consortium (a.k.a. W3C). On top of URI/URL, additional mechanisms of security and privacy features must be implemented to ensure cybersecurity as new technologies may introduce new risks. To reduce risk exposure, the OCA-compliant data administration agency should

[13] An well-known Universal Resource Identification (URI) and Universal Resource Locator (URL) scheme was invented by Sir Tim Berners-Lee, and the explanation of the two scheme's difference can be found here. However, the notion of privacy protection and security is not the first functional requirement of such system.

participate in the design and standards forming activities of cyberspace namespace management technologies. The technical standards of namespace management that is compatible with OCA-IS and OCA-DL will be referred to as OCA-NS.

5. ***A Cybersecurity research and educational content development workflow***: A content authoring and production team must work closely with the cybersecurity governance agency to create public-outreach content to ensure timely awareness of cybersecurity concerns. This team will follow a scalable workflow to develop educational material (OCA-EM) to inform casual users of public infrastructures, and train engineers and operational staff members who are responsible for developing and maintaining security critical infrastructure projects. This research and education team should also work with global security thought leaders and industry practitioners to introduce late breaking security assurance strategies and technologies. This research and educational content development team should utilize a Network-enabled Publishing Workflow[11] and an inclusive blended educational process[12] that integrates all facets of contributors to coordinate their digital assets and physical supply chain. This workflow will support a wide range of productive and creative activities that invites and guides participants to work and play. The workflow itself is also a channel of cybersecurity education that will help establish an equitable and generative social relationship in the global cyberspace, creating healthy dynamics that better preserve liveness and safety conditions of cyberspace operations.

OCA-Process for Cybersecurity Governance

The process of engaging an existing organization to practice sustainable cybersecurity protection is like ***shooting moving targets on moving vehicles***. The process to achieve cybersecurity governance must be designed by following the Principle of Information Symmetry. In the world of process modeling, the sequence of event occurrences, is the object of interest to keep symmetry. In short, OCA presents a meta-process model for cybersecurity governance with the following concepts in mind.

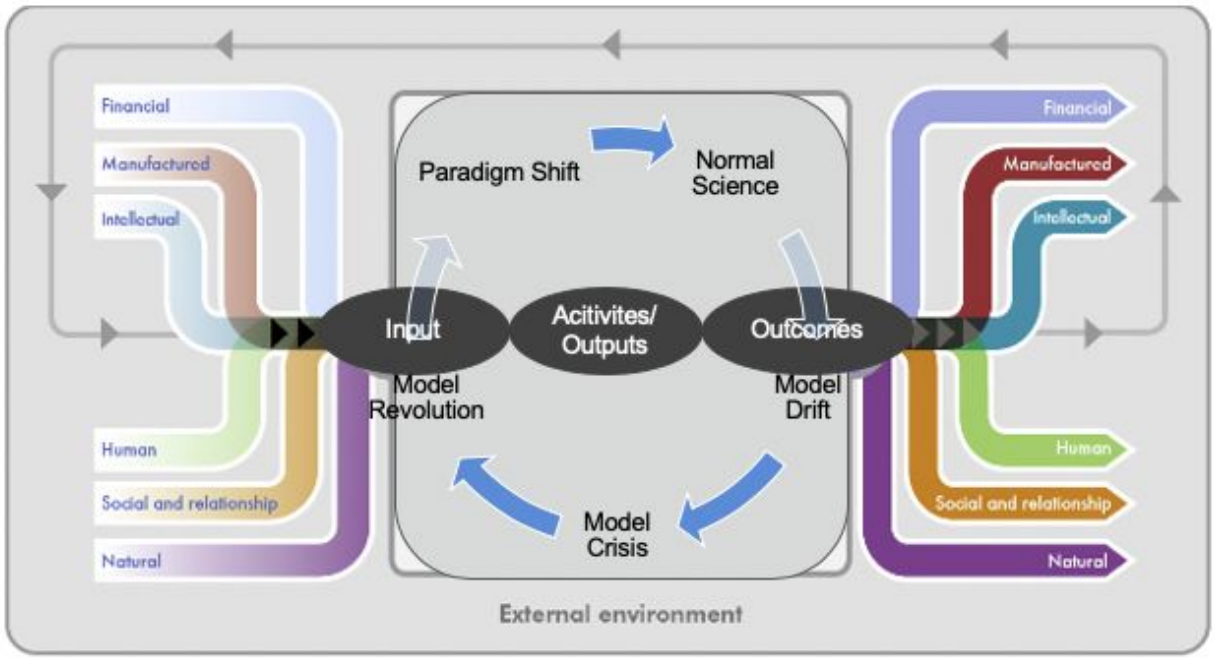
Avoid the trap: "Security through Obscurity"

When namespaces across the board are standardized, data privacy must be protected not through idiosyncratic naming conventions, but through adequate encryption protection. Using OCA-compliant process model to share operational insight through standard encryption/decryption mechanisms would systematically avoid exposure of organization's internal secrets. Based on the Principle of Information Symmetry, OCA deals with all crises and recovery opportunities in a uniform process model. A security-oriented, data-centric process model is all about time-stamped data. Therefore, process conformance helps historical records of previous cybersecurity attacks and solutions of other similar projects to be reused for future projects. To incentivize data and solution sharing, Open Source styled development practice is heavily encouraged. While private data content is protected under a secure process model, OCA considers Cybersecurity Process Solutions as a form of public goods, the process model should be shared and made available to all.

Process Integration across All Domains and Time Scales

A security-sensitive workflow should not hinder the normal progression of technology infusion. To be accommodating to technology advancements, OCA-compliant organizations should incrementally introduce updated security-aware tools and processes to their cyberspace partners that already have their own established cultures and operational regiments. OCA-compliance must be introduced through an evolutionary pathway, which incrementally adopts the unifying namespace (OCA-NS), that addresses people, space-time locations, and contractually encoded activities into a broader workflow pipeline. Within the pipeline, CICD/DevSecOps techniques are applied. The following diagram originally

designed for illustrating the Integrated Report system is a good visual representation of the same idea.



Modified from International <IR> Framework. Figure 2, p.13
http://www.theiirc.org/international-ir-framework/, accessed July 2020.

The Integrated Report diagram shown above is compatible with the philosophy of CICD/DevSecOps and most importantly, compatible with OCA. Having a unifying workflow pipeline, that combines the information flow composed of financial, manufacturing, intellectual properties, human resource management, social responsibilities, and natural environmental concerns. All these domains of operational information converge into a single workflow governed by a generalized system evolution process known as Kuhn Cycle[14] . The initial objective of introducing OCA-compliance is not just about rigid security guidelines, but the ability to inject process observability. As the diagram indicates, the Integrated Reporting model is congruent with the working principles of Information Symmetry, that all business activities are subjected to the "same" Governance Model. This diagram also reveals a visual symmetry that suggests a regulatory symmetry for an organization that takes all inputs and all outputs through a common security compliance

[14] The Kuhn Cycle is a process model of societal-level system evolution/revolution invented by Thomas Khun.

focal point. The inner cycle in this diagram shows that all controlling mechanisms over time must be sequentially refined without stopping the operation flow of the outer cycle in the "External Environment". One aspect of symmetry that this diagram didn't reveal, is the symmetry of information accessibility. An integrated reporting system should be presented to all relevant participants as transparently and conveniently as possible. As mentioned in the requirement section, OCA-compliance mandates the use of modern browsers to report and display operational data. In terms of cognitive convention of presenting data content to its users, the user interface, the layout and format of the data reports can be organized with the guidance formulated in the International Integrated Reporting Framework.

OCA-compliance promotes the use of a single, integrated naming and reporting mechanism to capture real-time operational data, and security status reporting data. Using a single, integrated naming and reporting mechanism across operational and security status reporting data allows consistent causal relation inferencing. The technical infrastructure required to manage both kinds of data is basically the same. Independent of the data content, presenting operational data and security status data via a unified human-machine interface further improves overall system observability, therefore, improving system-wide awareness[15]. Only through transparency and a unified data sharing platform, all participants can converge to a data-centric consensus. The Principle of Information Symmetry promotes consistency across all aspects of data formats and namespace management. The consistency also allows more technical practice, such as DevSecOps to be incrementally injected into the overall workflow. Since the same DevSecOps pipeline template, can be eventually shared by many, so that it can be expected that as the ICT industry matures, the organization that adopts OCA will be able to adopt new technologies at an accelerated speed without exposing its cybersecurity to uncontrolled risks.

Kuhn Cycle as a Meta Process for System Security

Thomas Khun, the science philosopher and historian, who's seminal work on The Structure of Scientific Revolutions[13], stated that the cyclic process of scientific discovery would inevitably cause systematic conflicts due to information asymmetry, which he introduced the idea:"model ***incommensurability***". When new scientific methods or technologies that are incommensurable to the parties in dominant power, then the governing system would

[15] The access rights for all participants should be managed by a single security assertion system, such as SAML[10].

be broken or exposed to the state of “model revolution”. From a cybersecurity viewpoint, this is a kind of systematic security breach caused by information asymmetry. As a meta process model, Kuhn cycle prescribes a specific sequence of evolutionary stages of all systems facing information asymmetry. The process of how information-asymmetries can be assimilated by society at large can be described in the following diagram:

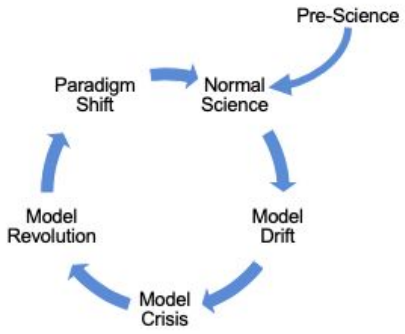
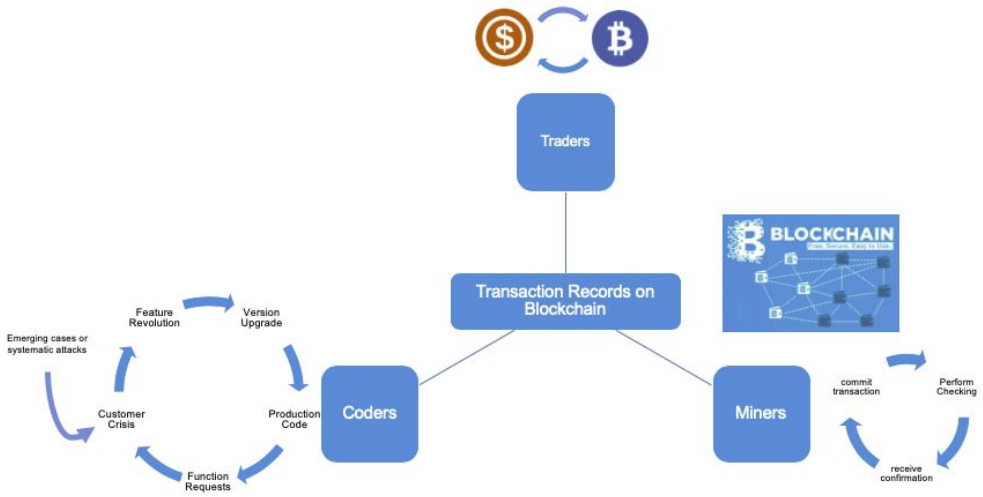


Image Source: https://www.thwink.org/sustain/glossary/KuhnCycle.htm

Since all systems updates and potential revolution is inevitable, designing a system that is free from intermittent crisis would appear unattainable. One may consider a counter-example, where Bitcoin/Blockchain-based socio-ecosystem[14,15] has a tripartite organizational structure. One may observe its ecosystem dynamics in the following conceptual diagram:



The Bitcoin operations inevitably involve three kinds of loosely coupled communities to mutually counterbalance each other. All three kinds of participants must agree on the data content of its double-entry bookkeeping[16] transactional records. This immutable[16] transactional data ledger is used by three parties simultaneously. The traders of Bitcoin or Bitcoin-like cryptocurrencies must record their transactions on this distributed, immutable ledger. Many copies of this "distributed" ledger are being monitored and checked by different miners. The performance of cryptocurrency mining technologies and the processing speeds of these transactions are regulated by volunteer coders. The coders are not directly paid by the Bitcoin reward system, partially because they can often purchase some cryptocurrency at early enough stages to guarantee long term profitability.

Three Different Time scales and the tripartite governance model

The above-mentioned three separate parties are mutually dependent on the others, yet their evolutionary time cycles/scales are significantly different. The traders operate on a transaction-by-transaction time scale, which is nearly continuous, sub-second time scale speed. The miners operate machines, they can only be rewarded after they effectively checked-in transaction records, usually organized in regular blocks of time, say 1 to 60 minute time scale. The coders would commit changes to the system, in ways that must pass many software and operational tests. This makes software update cycles facing many uncertainties, and therefore must take place with irregular time intervals. The difficulties in changing all three communities at once, is actually a safety mechanism for the overall health of Bitcoin operation. The Bitcoin community is one of the few global-scale financial transaction establishments that has proven to work for more than 10 years without a dominant organization or a human leader that actively maintains community governance. Bitcoin's legendary founder, Satoshi Nakamoto, is known by its secretive identity, and has thoroughly disappeared in the public almost immediately after its public release.

The key ingredient of Bitcoin's success is its tripartite governance model. This governance model inherently has the capacity to be fault-tolerant. This fault-tolerance is not only dependent on the Byzantine Fault-Tolerance of the Mining Machine Network, but also the functional complements of three separate communities that forces them to collaborate without having one party that can destroy the whole system at once.

[16] Immutable means once the data records are committed to the data ledger, it cannot be changed in the future.

Time is Money: Blockchain as a Socially-Verified Digital Clock

Clearly, there are deficiencies of Bitcoin's technical architecture that prevent it to be the Peer-to-Peer payment system for everyone. Since the public release of Bitcoin blockchain, many similar communities and technologies have been inspired by Nakamoto's ideas[17]. For example, to make it serve more transactions per unit time, it needs a very different infrastructure and a different participation model. In order to make "blockchain" programmable, so that it can be flexibly coded to serve many different applications, Bitcoin's data structure and the relatively slowly changing codebase cannot deliver the needed solution. Therefore, many new Blockchain/Bitcoin inspired projects started to have many totally different technical implementations. Effectively, these new code bases and new "public chains" are various revolutions in the Bitcoin community. Even the original Bitcoin blockchain has branched out into two separately maintained chains of transaction records. The only overarching principle that enabled these loosely coupled communities to continue working together, is the Principle of Information Symmetry.

Timestamps as a Source of Truth

For all these communities to survive and thrive, the fundamental governing principle cannot be changed. At any moment, when any one of the three mutually dependent communities stop sharing the same, symmetrical transactional record data, a "Hard Fork" occurs, and two sets of participant accounts must be maintained into the future. Even under "Hard Fork" situations, the timing of the forking event is being witnessed by all traders and miners, and up to that point, all time-stamps that are associated with all transactional records can still be considered to be "trust-worthily" correct between the two forked branches. It is this ***trust-worthy time-stamp*** that is the main source of truth that grounds the data assets for the governance model. Blockchain's design is about using many independent parties of interests, to collectively witness the occurrence sequence of a long chain of events. As the chain gets longer over time, more events would have been verified, and therefore become more "trust-worthy" than other chains that only have a short time window to reflect the mutual verification relationships between events. The strengths of trust-worthiness of time-stamp systems are measured by the length of its blockchain, and the lengths are how different blockchain-based systems could measure and justify its social

value and therefore why blockchain with longer history is usually worth more than short ones.

Defining Security Risks via Khun's Namespace

The Kuhn cycle can be thought of as a process-oriented namespace to assign semantically meaningful labels to security risks. The following table presents a set of typical terminology that are used in Kuhn cycle, software engineering, and namespace management.

Khun Cycle Classification	Software Engineering	Namespace Management
Normal Science	Production Code	Current version number
Model Drift	Operational Error Cases	Error Case Sequence No.
Model Crisis	User Complaints	Complaint Classification
Model Revolution	System Downtime	Hard Fork Label
Paradigm Shift	Software Replacement	New Version Release

By thinking of the Kuhn cycle stages as system risk classifications, applying modern data management techniques to manage these labels of risks in an organization-wide namespace, it is effectively a way to manage organizational knowledge about risks. In fact, as long as data storage is sufficiently abundant, all events, regardless of whether they are physical or purely informational, can be given unique names. Systematically organizing names around certain subject-oriented names, such as security-oriented data semantics would actually instill security-sensitive meaning to these assigned names. Independent of the subject-orientation, all event occurrences can be registered as instances of data record associated with certain other events through their time-stamps.

The Causal Structure of Assigned Names

Trust-worthy time-stamps provide an implicit, yet ***universal causal structure*** across all temporally-labeled data records. Knowing that time-stamps associated with Blockchain-like transactional records are witnessed by many parties, the time point of transaction occurrence is difficult to fake, and the blocks associated with these transaction records are given unique and unpredictable labels/names. These labels/names can be bound to other data sets to indicate the time of data entry. Therefore, many kinds of data sets can be

related through time-based labels. To reason about what events have impact on system security, the sequence of event occurrences can be computed to identify causal dependency, therefore allow investigative efforts to reach into temporally-related data sets to identify the possible causal structures of attack. Combining the security semantics as prescribed by Khun, and relating all the operational data content of a security sensitive system with a Blockchain-like digital clock, the names given to security related events would be supported by the temporal sequence information to construct historical operational data with certain accountability. Referencing the historical data with publicly-known events would further enrich the possible causal structures that might lead to past and even future security breaches. This time-based approach to instill trust-worthiness in data is a major resource that can be leveraged in organizational governance. The time-stamps of many seemingly irrelevant events implicitly constructs a causal network that can be utilized to inform decision-makers. The inferred causal structure through time can also be used to identify the root-causes of security breach, and potentially solve the security problem systematically.

The Statistical Process of Security Knowledge Management in OCA-NS

By using Blockchain-like datastore to capture operational data of a cyberspace system, and associate these data in a security-oriented namespace, one may create a dynamically updated cybersecurity namespace for an organization. This namespace can also be further processed to be shared with other similar organizations to create a knowledge base for solving cybersecurity problems across organizational boundaries. The process of creating and sharing namespaces, knowledge bases, and security response services, are literally identical to an industrial strength data center operation, and it has already become a “normal science”. The namespace defined for security related knowledge will be stored and published through the knowledge content of OCA-NS-SEC, where NS stands for NameSpace, and SEC stands for security. To access OCA-NS-SEC, all OCA-compliant information systems can use OCA-IS to query and share this growing knowledge base.

Statistical data on newly popularized terms can reveal security risks

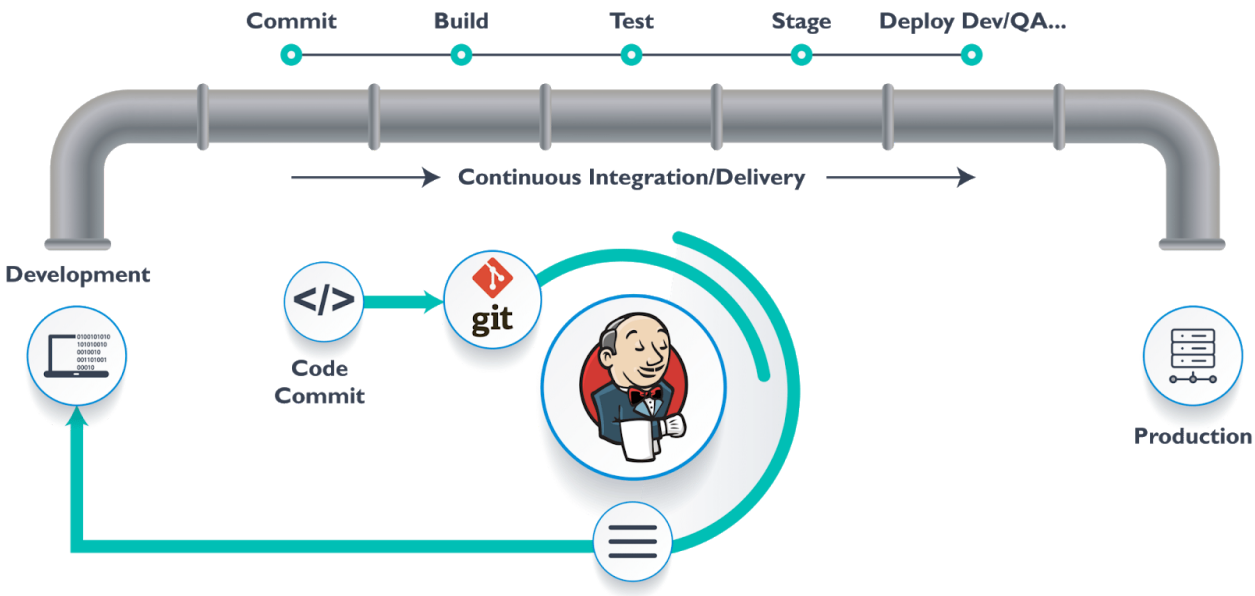
When new buzzwords start to appear in public awareness, they signal a wave of societal “model drift” which in turn implies that some eventual “model crises” are looming. The statistical indicators of buzzword usage can be systematically detected from popular search

engine statistical data, such as Google Trends. In private organizations, the frequency of new buzzword usage can also be measured using data analytics functions in popular digital workflow service platforms. For example, Service Mesh Platform tools, such as Istio, Consul, and Linkered are technology solutions that can detect the frequency of buzzword usage, which could signal structural revolutions in Kuhn Cycle. Using a more recent example, the term: "Covid-19", would have been totally incommensurable by anyone living in the year 2019, but now, it is a common term used by everyone. Not only it became a commensurable term to all, it also forced many nations to practice the "New Normal" social distancing policies. In software engineering, the management of "paradigm shifts" is by introducing new versions of software. It can also be managed by introducing new extensions or a different software product line. In any case, there are signs that could be systematically detected to prepare a system for potential crises, revolutions, and paradigm shifts. In summary, tracking the occurrence frequency of currently "incommensurable" terms can be a practical way to detect and measure system-wide security risks.

The Speed to Sanity: The Velocity of Paradigm Shifts

The popular appearance of incommensurable terms is only a signal to system crisis. Having signs of a potential failure doesn't equal to failure itself. If a cybersecurity system can react quickly to emerging threats, it will reduce its exposure to cyberattacks. However, to fix the gap caused by incommensurability, simple knee-jerk reactions will not solve the problem. As spelled out in the Kuhn Cycle, the revolutionary cycle must go through multiple stages to reach normal science again. Each of these cycles must include a Paradigm Shift, which can be analogously related to an official version release of a technical system, such as Operating System upgrades.

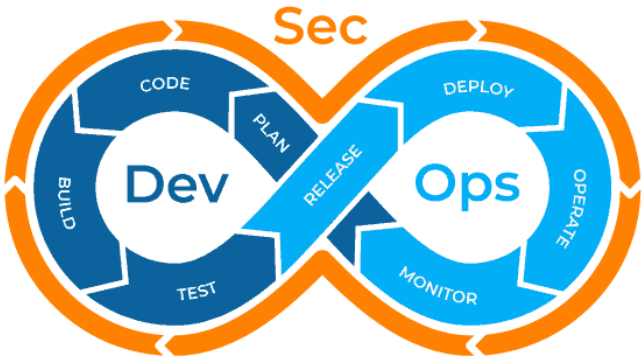
To make sure that the system is resilient to attacks, the simple solution is to make the cycle time small enough to quickly release technical patches in ways that minimize the system's exposure in the crisis mode. This approach is now generally called: CICD, also known as, Continuous Integration and Continuous Delivery/Deployment. CICD is often organized as a pipeline or one continuous workflow. It can be illustrated in the following diagram: (Image courtesy of DevOps Zone)



The main feature of CICD, is to automate the development to operations pipeline as much as possible. Once new code changes are committed, they will trigger relevant build, test, stage, delivery, deployment activities automatically. In most cases, automation could minimize the idle time between different collaborating departments. However, increased speed and frequency of product deployment could also introduce new sources of errors. One must ask:

What if the testing and staging procedures didn't catch critical errors in the system, and caused unexpected, or even intentionally injected errors to the system?

Speed increase can be a source of security breach, and therefore, DevOps/CICD, not only requires a highly disciplined product development organization, it also needs to embrace security practices at all stages of product development, deployment, and maintenance activities. Overtime, this security-awareness practice gave birth to DevSecOps[18, 19]. On the highest level, DevSecOps can be understood as an extension to the infamous DevOps Logo shown as follows:



This DevSecOps logo reveals that DevOps is an iterative cycle of eight distinctive subprocesses, while security wraps around all of these eight subprocesses. It simply means that security verification practices must be incorporated into all stages of development and operations activities. The first condition for OCA-compliance is an based on DevSecOps's "security first awareness" philosophy.

Distributive Justice: Security on top of DevSecOps

To systematically maintain cybersecurity protection, there are a few more layers of security concerns that go beyond the scope of DevSecOps. First, to expedite the Development to Operations cycle, incorporating security checks and verification policies requires additional tooling for process automation. These additional automation and tool insertion requires qualified security experts to invest significant time and efforts to create adequately secured development pipeline. Therefore, DevSecOps may not be affordable by small organizations or developmental projects without dedicated cybersecurity budgets. This is an area that creates asymmetric advantage for large and well-endowed projects. As small products grow in functionality and capabilities, they could eventually become an influential product/service without sufficient built-in process security, and therefore threaten the overall security of the cyberspace of public interest.

Second, since CICD/DevSecOps development practices are enabled by highly skillful ICT professionals. These skillful ICT professionals have based on their skills to create many branches of competing methodologies, commercial services and proprietary software that each does CICD/DevSecOps better in different areas of work. To implement a large, critical

public infrastructure project, it is often necessary to adopt almost all of these different methods and tools. As the number of methods, tools, and services continue to grow, the complexity of managing these potentially incongruent methodologies, tools, and services can be overwhelming. Therefore, a theoretically sound and complete framework, that can subsume all the methods, tools, and services into one common system, is almost the first and foremost task for all large projects. Having access to globally reputable industry standards organizations, such as IETF, IEEE, IEC, and government agencies that promotes education on cybersecurity awareness would be an indispensable condition to create sustainably large, critical infrastructure projects. These organizational processes should be constantly working with different security experts, global industry standard organizations, suppliers of cybersecurity solutions, and CICD/DevSecOps solution providers, to ensure constant updates and to participate in the discourse of future cybersecurity trends.

Last but not least, most security issues are known to be hacked through social engineering. Hackers and cybersecurity experts would most likely agree with the following statement:

The social-trust network is almost always the weakest link in a system, therefore, the easiest way to hack, is to hack through social engineering.

Assuming that technical systems are designed with flawless logical integrity, if the owners of the system willingly or unintentionally breached the security protocol, all of the above mentioned protection mechanisms would not have much use. Therefore, from a technical viewpoint, the least trust-worthy persons are actually the controlling members of the system, because these powerful operators could either induce operational errors when conducting critical authorization operations, or they can potentially misunderstand the technical implications of their actions. To minimize the overall risk, there should be many more people each controlling a smaller portion of the overall system. Colloquially, one may say: "***Don't put all eggs in one basket.***".

This strategy can also be associated with the notion of Distributive Justice. Knowing that humans make mistakes is not a judgement of ethics, this is a technical statement based on the Theory of Distributive Justice, another way of stating the Principle of Information Symmetry by legal scholars[20]. A typical technical solution is to choose a security model that minimizes exposure of major security holes to a few selected individuals in the whole system. The question arises, what kind of security model is trust-worthy?

The Management Process of Trusted Namespaces

Most Internet users would inherently trust the uniqueness and transparency of Email addresses(partially based on DNS), DNS (domain-name services), and IP Addresses (IP stands for Internet Protocol) for connected devices. These Internet-age identities for humans and machines are used as automatic identification mechanisms to authenticate and authorize data exchanges. For example, when you lost your password, usually the system would send the "reset password" email to your previously registered email address. These Internet-wide namespaces, whether it is email accounts, IP addresses, or Domain Names, are considered as private properties whose controlling rights can be transferred by certain namespace management agencies. Controlling these unique and publicly known names is the strategic controlling point for the Internet. The managing principles of these "naming" services can be leveraged to create other cybersecurity systems. In addition to OCA-NS-SEC, OCA presents three basic types of naming services: digital credentials for account identities(OCA-NS-ID), standardized names of Space-Time Locations(OCA-NS-STL), and the contract names of Automatic Contract Execution(ACE) systems. The OCA-compliant Namespace-Management Process (OCA-NSP) defines the update mechanisms of these trusted namespaces.

Namespace Management for Human Agents and Agencies

When working with legacy systems, the identities of human agents and agencies are managed in a sub namespace of OCA-NS, called OCA-NS-ID. OCA-NS-ID will adopt existing authentication(AuthN) and authorization(AuthZ) technologies. Initially, SAML will be used as a tool to integrate existing AuthN/AuthZ infrastructures. Existing AuthN/AuthZ technologies can be broadly classified into three major paradigms:

1. Centralized Trust: A single, centralized organization provides the authentication and authorization services.
2. Federated: There are a few existing protocols, namely Open ID, OAuth, and SAML that use a third party Identity provider or identity providing consortium to provide authentication and authorization services.
3. Peer to Peer Model: A Self-Sovereign Identification (SSI) model, this model allows two parties to directly authenticate themselves or authorize certain transactions

through a common distributed platform run by a large number of anonymous participants. This model is becoming a popular solution after Bitcoin/Blockchain became available. However, SSI does not always have to use Blockchain technology, technology that can be reliably run by a large number of anonymous participants can provide the support to SSI.

The pros and cons of each security model can be found in various literatures[21, 22, 23]. The first two identity models rely on an asymmetric trust relationship that involves a redundant third party for symmetric transactions. Only the third category, SSI utilizes a symmetric trust relationship. Therefore, whenever possible, OCA-NS-ID prefers the SSI model over the other trust models.

Namespace Management for Physical Space-Time Locations

OCA-NS-STL represents the namespace of space-time locations of our physical world. Given some mathematical convention, it is technically trivial to have succinct names that refer to all physical locations in space. For example, What3Words, a spatial location naming service, assigns a 3 words natural language phrase, each relates to a specific 3 meter-squared location on earth surface. As of now it supports 44 natural languages, including Arabic, Bahasa, Chinese, Dutch, English, and many more. This simple word combination can be translated to an exact longitude and latitude location on earth. This universal translation from words to spatial location can be used by any emergency agencies and even national defense operations. (Picture credit: What3Words.com)

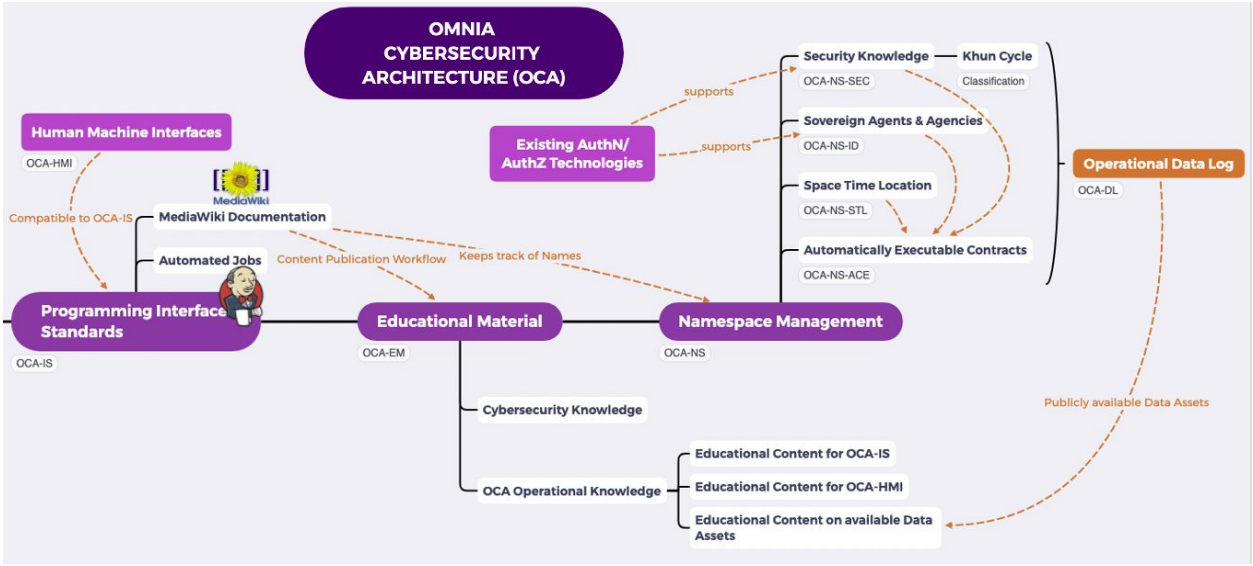
Data services that establish globally accessible naming conventions could be useful for many social and economic applications. As Web 3.0, Spatial Web[24] and Blockchain-inspired technologies become more popular, globally accessible name services will provide a data-oriented space-time framework that defines the named boundaries of our cyber-physical space. Allowing the general public to have free access and verify the correctness of these namespaces is one necessary condition to make these services trust-worthy. Having an inclusive process to manage the globally accessible spacetime namespace is the technical challenge of operating a globally equitable cyber-physical space. Moreover, a globally accessible, trust-worthy data service that defines the publicly recognizable names of spatial and temporal locations is a starting point to integrate cyber security with physical security. The data service on spacetime locations will also be an foundational element for the construction of many public infrastructure projects, such as Smart City, Emergency Response Systems, National Defense Systems, and Global Supply Chain Management.

All of these applications should share a common spacetime location (STL) naming service substrate whenever possible, namely OCA-NS-STL. The time increments in the global physical space can be time-stamped by a blockchain-like digital clock, so that the trust-worthiness of the time-based namespace can rely on features of blockchain as mentioned earlier. The namespace of spatial locations should also be managed by a blockchain-based version update mechanism, whose updated versions are given trust-worthy time-stamps generated by certain publicly accessible blockchain, so that the timestamps cannot be easily tempered. The update records of spatial data will be associated with user accounts, whose user identities are managed by OCA-NS-ID. This data update management mechanism will allow changes made in OCA-NS-STL to be accountable to individual participants in the OCA-compliant user account management process.

Trust-worthy Namespace makes Automatic Contract Execution Smart

Smart contract technology is a kind of Automatic Contract Execution(ACE) system. It uses the distributed computing ideas in blockchain to “guarantee” automatic execution of written contracts. However, to execute written contracts in spacetime contexts, a publicly agreeable namespace for spacetime, such as OCA-NS-STL, becomes a necessary vocabulary standard, Once the identities of human agents, and the publicly accepted names (labels) of

space-time locations can be digitally referenced, it would be particularly convenient to construct socially agreeable contracts. The namespace OCA-NS-ID, would systematically assign identifiable accounts to humans or human agencies. The physical space-time locations labeled OCA-NS-STL, can encode the timing and delivery status of product/service transactions. OCA-NS-ID and OCA-NS-STL are formatted data to help define digitally verifiable contracts. Once a version of the contractual agreement is created, the execution history of the contract, and the spatial locations of relevant assets to be transferred, can be described in an OCA-compliant namespace system. Knowledge about the latest status updates in an OCA-compliant digital contract, is the real time knowledge about the digitized value supply chain. In certain cases, people can use these historical data about these digital contract executions to assess the credibility of the participants, therefore the historical data can also have significant economic values. The contracts that have been proven to work at scale, can also serve as contract templates for different, but similar business operations. Automatic contract execution systems can be particularly valuable when it works with a trust-worthy namespace that incorporates human agencies, spacetime locations, and executed contracts with significant operational history data. It is the trust-worthy namespaces and historical data content that make ACE smart. The following diagram illustrates the relations between Programming Interfaces, Educational Materials, and Namespaces in a hierarchical manner.



In modern ACE systems, Ethereum (ETM) would stand out as the dominant implementation amongst a few other competing ACE systems such as Cardano and QTUM. All these ACE systems or “Smart Contract” technologies need a consistent namespace management standard. OCA-compliant namespace management scheme would provide a consistent policy to name all these contracts, spacetime locations, accounts, and resources using a single naming convention. The consistency in namespace management could therefore enable a certain level of interoperability across many existing ACE systems. This namespace would allow executable contracts to be encrypted under proper privacy protection, and searched by users to review historical contractual execution data when needed. This universal naming scheme follows the software engineering principle often promoted by Service Oriented Architecture (SoA), and the vision was pioneered by the World Wide Web, and partially realized in the form of Universal Resource Locator(URL)/Universal Resource Identifier(URI). In the era of Web 3.0, or someone would call it: Spatial Web revolution, a unifying naming scheme that addresses human agencies, space-time locations, and version-controlled executable contract is a natural extension to the idea of CICD and DevSecOps at a scale that could serve the entire Cyber-Physical Space of a long time to come.

Required Resources: Enablers for OCA-Implementation

To start the implementation process of OCA-compliant cybersecurity practice, one would need three major categories of resources:

1. ***Resourceful Participants***
2. ***Management processes enabled by CICD/DevSecOps***
3. ***Enabling Technologies***

The participants are to be classified and named in a unifying data scheme, so that they can be eventually governed under an OCA-compliant participation model. The current management practices are to be redirected to an OCA-compliant process model, so that the entire organization can incrementally adjust their culture to become security aware as new technologies challenges their prior impression of security awareness. Last but not least, as new enabling technologies appear on the horizon, an OCA-compliant workflow can define and adequately subsume the functional roles of these new technologies into adequate security policies.

Participation Model: How to engage and disengage participants

User Base:

To manage participants in cyberspace and hold them accountable for their actions, it is necessary to use a scalable model of identity management to serve the cybersecurity needs. There are many existing Internet-scale Identity Management Models[25,26], namely: Centralized Identity, Federated Identity, User-Centric Identity, and Self-Sovereign Identity (SSI). Abiding to the Principle of Information Symmetry, OCA preferentially adopts SSI over other Identity management models to maximize inclusivity. The rationale in why SSI is adopted can be found in Christopher Allen's "The Path to Self-Sovereign Identity" [27]. Access rights to all user account systems should be encoded using an extensible security assertion model. Known solutions such as Secure Assertion Markup Language (SAML) can be adopted as the initial solution.

A broad range of participating users that might be included in a publicly accessible digital publishing workflow. One possible user classification can refer to Wikipedia's participation

scheme. For example, in Dariusz Jemielniak's book[28], the roles of Wikipedia community is divided into the following categories:

1. Steward
2. Check user
3. Oversigher
4. Bureaucrat
5. Administrator
6. Rollbacker
7. Registered user
8. Newly registered user
9. Unregistered user
10. Blocked user

Independent of their functional roles in a generalized digital publishing workflow, they can all be assigned different levels of data access rights, using a common programmable language, say SAML.

Cybersecurity Administration Staff:

The operation of OCA-compilant critical infrastructure would require multiple dedicated professional cybersecurity staff members to plan, execute, and maintain the health conditions of infrastructure cybersecurity. The skill requirement is that the composition of these professional staff must cover the knowledge base of cybersecurity protection operations, and large-scale system design and management. The function of system design and management expertise is to enable integration and reconsideration of incorporating ICT capabilities into traditionally non-ICT intensive infrastructure projects. While Cybersecurity expertise will be utilized to design, test, and deploy security services to the infrastructure projects, high level system design and management staff will work at defining long term deployment plans and identify system integration opportunities that require dedicated investigative and coordination efforts. In most cases, this Cybersecurity Administration Team ***should not exceed the number of 7 people***.

International Industry Standard Organizations

The field cybersecurity is developing rapidly, but still in its infancy. The possible ways to attack a cyber-physical system is expanding rapidly, much faster than any independent agency or technology supplier can manage to cope with its complexity. Moreover, many new application areas and use cases are still to be invented, therefore, the boundaries of what is considered to be cybersecurity are not fixed. As mentioned earlier, social media hacking and social engineering can be considered as an important branch of cyber-security, but comprehensive remedies have not been formulated. To formulate industry standards based on solid operational experience and publicly witnessed events and data sets could significantly improve the trust-worthiness of security practice at large.

Therefore, the OCA-compliant process model will encourage all stakeholders to actively participate in the shaping of industrial standards. Cross Disciplinary boundaries are particularly fruitful in defining new standards, particularly in the area where Machine Learning, AI, and data intensive application that relates to cybersecurity. This is a fertile ground to get involved in the earliest stage. The areas covering security policy-making, cybersecurity law, universal data access rights, and cyberspace-related ethical concerns are active domains that already have existing industry standard organizations and technology consortiums that work on these topics. The following list is an incomplete list of key industry standard organizations (ordered alphabetically):

1. CNCF: Cloud Native Computing Foundation
2. CXI: Council on Extended Intelligence
3. IEC: International Electrotechnical Commission
4. IETF: Internet Engineering Task Force
5. IEEE: Institute of Electrical and Electronics Engineers
6. ISO: International Organization for Standardization
7. Linux Foundation: The Linux Foundation
8. NIST: National Institute of Standards and Technology
9. OASIS: Organization for the Advancement of Structured Information Standards

A Brain Trust that performs Research and Development

Cybersecurity is an area that evolves at a pace much faster than other industries. Therefore, it is necessary to keep advancing the knowledge and refreshing the strategic understanding of current cybersecurity affairs.

To keep an organization thriving at an industry leading position, a solid brain trust, where a balanced composition of multi-disciplinary experts can continuously challenge each other is a necessary strategic investment. They need to continuously advise the leaders of the protected organization about the late-breaking enabling technologies, risks, and developmental opportunities at the earliest possible time. This team of brain trust should also be composed of not only security experts, but also data scientists, network and computing infrastructure architects. A succinct description of this functional team is shown below:

A team composed of cybersecurity experts, who can act as, or work with the following types of domain experts:

Accountants, Business Leaders, Data Scientists, Economists, Government Agents, Hackers, Historians, Journalists, Law/Policy Makers, Linguists, Telecommunication Operators, and User Experience Designers.

These experts may contribute to this brain trust through a digital publishing workflow that is OCA-compliant. To ensure inclusivity, anyone who is insightful in observing the cultural, historical, and philosophical aspects of societal evolution should be invited to contribute to advance the work of this brain trust. The governance and incentive model of this brain trust should be consistent with the Principle of Information Symmetry. The contribution of all participants should be recorded using a data-intensive contribution accountability management system.

Use OCA-compliant Educational Program to raise Security Awareness

Up to the time of this writing, DevSecOps and CICD is still only being practiced in rather elite software development communities. However, in the ever accelerated Cyberspace arena, time is not only money, the ability to procure the best practice also significantly advances the security awareness and automation capability of a civil society. The best

defensive strategy is to embed security awareness at all levels of daily information exchange operations. This really means all citizens in any modern society. In other words, the Principle of Information Symmetry should use an OCA-compliant process to educate the public, so that this publishing workflow process can raise the cybersecurity awareness of all people. Knowledge is power, the ability to continuously introduce information and cybersecurity literacy through a common educational process model pioneered by CICD/DevSecOps can be particularly beneficial to early adopters. OCA-compliance should be introduced to educational administrations of the public, so that organizations and individuals can start being informed about, and start practicing these advanced civil rights provided through enabling technologies. A truly secure society is a cyber-physical space that ensures universal equity on a societal scale, no one should be left behind. OCA-compliance should be continuously taught to all age groups and all professional levels.

Future-proof Infrastructure and OCA-compliance

Most modern organizations are already entrenched in ICT-enabled process automation technologies. Once any user uses his/her phone to order food, call for taxi, or book hotels, a globally spanning workflow would be triggered to action. The power of cyber-physical infrastructure is not at its complexity, it is the simplicity that encroaches into our daily lives that present the deepest security concerns. As of today, the issue of cybersecurity is not one of technology scarcity, it is the overwhelming speed of technology infusion controlled by external interests that post imminent security threats. Most people and organizations simply have no way to reason about what these new technologies have done to your data already.

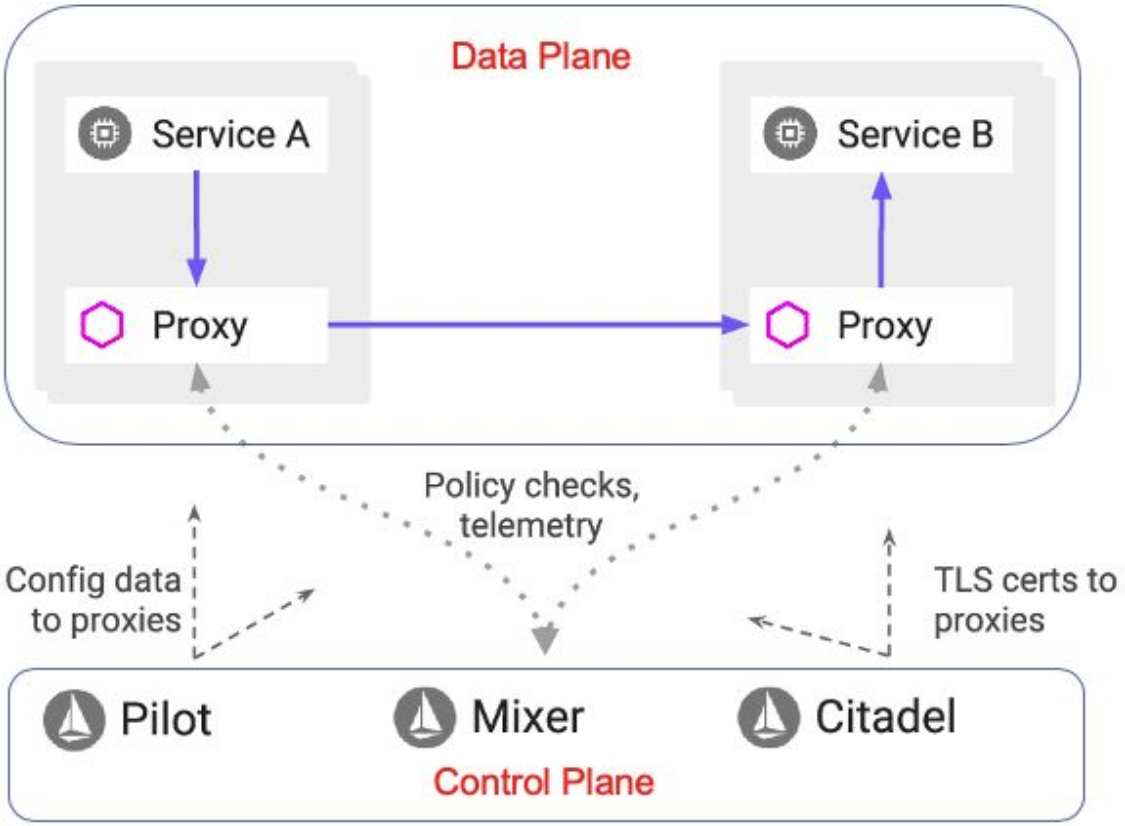
Racing against time: Maintaining a future-proof system with current infrastructure

According to the Principle of Information Symmetry, the best kind of change is action that avoids unnecessary changes. System infrastructures built in the past, may or may not have sufficient consideration to be future-proof. New technologies often introduce security concerns that break an existing working system, so that changes become necessary. Fortunately, a new breed of system integration platform called Service Mesh can help modularize the security attack surface, and help expedite technology infusion processes with a consistent security model in mind. The overarching benefit of Service Mesh is its

ability to avoid unnecessary change, so that it reduces system downtime or expedite technology infusion caused by changes.

Service Mesh as a Industry Standard: Structural Symmetries in Data and Control Planes:

To introduce OCA-compliant security concerns into an existing, open-ended cyberspace infrastructure, it is possible to adopt Service Mesh, as a consistent way to decouple controlling, organization-wide business logic from feature-rich data services. The notion of Service Mesh technology platform basically separates all cyber-physical systems into two planes, the Data Plane and the Control Plane.



Modified from Getting Started with Istio on Amazon EKS
https://aws.amazon.com/blogs/opensource/getting-started-istio-eks/, accessed July 2020.

As indicated in the diagram above, all data that moves across any two devices are monitored by the same software, called Envoy. An Envoy, a.k.a. Proxy, serves as a gate-keeping intermediary placed next to each of the participating data services. Once all of the data services are abstracted into compositions of Envoys/proxies, these services can be

combined, and routed together to deliver a wide range of complex business services. This uniformity of adopting one kind of standardized proxy to manage all data services, is a kind of “data structure symmetry” that unites all services into one common data plane. The security model of all data assets transferred on the data plane is managed by one unified controlling mechanism, called the Control Plane. A control plane is composed of Pilot, Mixer, and Citadel, which are three centrally configured agents that direct and authenticate proper data movements between “envoys” acting in the data plane. This unification of many existing services through the introduction of “service mesh” management has been a major movement in recent ICT infrastructure deployment. Many large scale Service Mesh platforms, from Netflix-like on demand video delivery, to global supply chain management and e-commerce logistics that reaches hundreds million end users have been implemented and operated for a few years in the industry. The lessons that ICT industry learned from deploying Service Mesh technology can be broken down to three folds:

1. Legacy ICT infrastructures can be wrapped around proxies/Envoys and then integrated using Service Mesh.
2. Service Mesh allows a system to introduce a consistent security model using the Control Plane.
3. When guided under a principled approach to system integration, new and old data processing services can be implemented in a consistent and incremental fashion, so that existing operational infrastructures can be subsumed into the new security model overtime.

It is the flexibility and inclusive nature of Service Mesh integration that demonstrates the power of Structural Symmetry. By standardizing on one Envoy-compliant data format and one control plane to orchestrate a seemingly unbounded system, arbitrarily complex systems can be incrementally combined, and channel the power of data flow control toward a single control plane. Service Mesh is a proven software engineering technique to cope with ever-increasing complexity of cyberspace system integration. Other related technologies, such as Solid of Inrupt Inc. initiated by the inventor of the World Wide Web, Sir Tim Berners-Lee, is also a technology that is based on giving more choices to all users to own data in a more symmetrical manner.

Service Mesh helps migration from existing workflow to OCA-compliant workflow

Service Mesh is an enabling platform, a layer of ICT plumbing that has proven to work at scale. However, Service Mesh implementation doesn't guarantee overall system security[17], it only provides the convenience to introduce a single security management tool via the Control Plane. For existing ICT resources that are not security sensitive, exposing them through Service Mesh would be a natural choice. It enables a level of flexibility and compositionality, that allows anyone to recombine data services through one consistent data management platform. In many cases, introducing the Service Mesh platform allows an incremental approach to flexibly choose existing ICT workflow practices to match OCA-compliant standards.

In comparison to retrofitting existing ICT infrastructure to Service Mesh platforms, it is more robust to start new organizations from a clean slate. Constructing a system from the software/hardware components originally designed for Service Mesh could reduce inconsistent security models that already exist in many separate, legacy systems, whose innate logic for security may not fit the Service Mesh platform.

Utilizing Open Source Solutions to replace Similar Functionalities in Existing Systems

Another route to transform existing ICT infrastructure to practice OCA-compliant security infrastructure is to identify functional capabilities of existing ICT services and replace these services with Open Source solutions. Due to the breadths and depths of Open Source solutions, most popularly known ICT capabilities ranging from Customer Relations Management, Supply Chain Inventory Tracking, Geographical Information Systems, to Video Conferencing tools, have all been made available in both binary and source code form. By identifying replaceable functional areas in the legacy system, and using the code base provided by the Open Source community, could significantly expedite the speed to reach OCA-compliance.

Data Migration: The Legacy Asset

The only thing that is not replaceable is the historical data. To migrate existing data sets to new systems should not only be done through manual coding practice, automated data

[17] Security holes in the original data services, especially physical security of the overall system might not be covered by a unified control plane.

migration tools should be used. There are well-known formal method supported practices to migrate legacy data. Security-sensitive data migration practice is also one aspect of OCA-compliance, and should be managed accordingly. In theory, data migration processes should be conducted through a form of encrypted, or zero-knowledge testing, verification, and deployment mechanism. Ideally, all data content should be backed up and encrypted to protect content security and anonymity. This requires a much more involved engineering effort that cannot be achieved through recombining a legacy system. Therefore, OCA-compliance at the higher levels would require a packaged implementation, and the open source nature of OCA-compliance could allow secure data management capabilities to be shared across many organizations, therefore minimizing the entry-barrier to organizations that cannot afford to implement the whole system from scratch.

Working with existing ICT Methodologies: CICD/DevSecOps

Operating cybersecurity-aware ICT infrastructure requires experienced and well-documented case studies. Continuous Integration, Continuous Delivery/Deployment, and DevSecOps as mentioned earlier are significant knowledge repositories of these operational experience and case studies. A significant expert community also exists to help develop these methodologies further. OCA-compliance is also based on these prior arts and encourages OCA-compliant organizations to study and work with CICD/DevSecOps experts.

Enabling Technologies for OCA-compliance

To continuously support the implementation and sustainable operation of OCA-compliant cybersecurity system, the following enabling technology components must be incorporated.

1. Automatic system composition and verification toolchain
2. A knowledge collection, storage and search engine
3. A workflow execution agent integrated with the knowledge engine mentioned above

The functional roles of each of these technologies are explained below.

Security awareness must work with systems on a compositional level

A resource-intensive hurdle in gaining confidence about system security is about collecting real-world operational data. A system is validated only by having collected sufficient real world case studies. Cybersecurity attacks are often conducted under a clever mix of circumstantial conditions, that all of which combined created effective damage or penetration that were unbelievable before it actually happened. Without a scientific approach to model compositional effects of interactive scenarios, the case studies of cyber attacks can only be documented in terms of cyberspace story-telling or case-by-case anecdotal descriptions. Testing data, formal proofs, simulated scenarios are just theoretical hypotheses. However, running tests in real world application contexts can be overwhelmingly dangerous. For example, certain military or medical applications may not allow real world trials. The only possible way to try as thoroughly as possible, is to create a toolchain[29] that can associate all available operational data, so that real world data can be composed to emulate a desirable scenario.

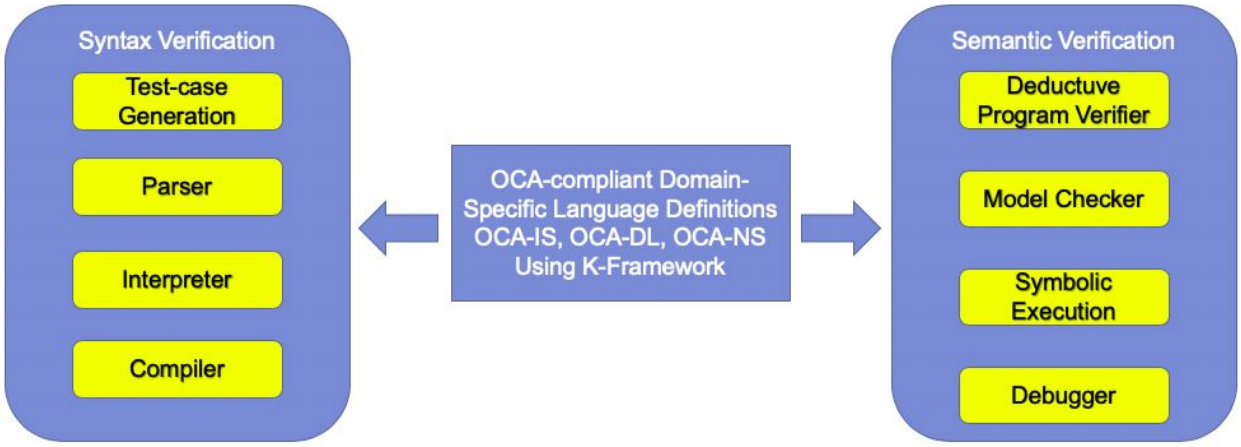
A toolchain designed to manage namespaces

To create such a composition and system verification tool, one must utilize software engineering and data manipulation tools that can work across multiple levels of system abstractions[30,31]. Choosing a general purpose, yet highly integrated system verification toolchain as the foundation for tests and verification can significantly reduce the application-specific software engineering work prepared separately.

Thinking across multiple levels of system abstraction requires both theoretical computing science knowledge and practical, battle-field tested software engineering tools. From the viewpoint of theoretical computing science, all systems can be represented as some formal languages, and the syntax and semantics of languages are the elements that represent compositional patterns. Using meta-language tools, such as K-Framework[32] to model security patterns enables security-related knowledge to avoid premature lock-in to a particular collection of technologies. In an extensible linguistic framework, all things and systems can be named and interpreted in additional layers of abstraction. One may consider the following axiom as Omnia's principled security approach:

Omnia considers formal languages as units of abstraction to organize and test compositional hypotheses.

Based on this axiomatic assumption, Omnia needs to use a language construction and verification toolchain. Just like K-Framework is about formal language analysis and design, LLVM, Coq, and Agda are some of the few formal verification and language engineering toolchains that are fully open source and have significant learning and teaching material for industrial strength programming languages. After certain comparison, we consider K-Framework to be OCA's starting point to represent security knowledge and construct security protection tools. The following diagram shows the integrative feature sets that K-Framework can perform on formal languages.



The diagram above shows that tools or functions of K-Framework can be language-independent. These analytical tools and compositional functions can be applied to any "languages" or "knowledge representation formalisms". This again echoes the Principle of Information Symmetry, that choose a design decision based on some form of generality or invariance. Applying K-Framework explicitly in the application context of Cybersecurity analysis and verification is about directing the mindset of cybersecurity experts to organize security problems as formal language design problems. This language-oriented problem formulation could better capture the compositional nature of security, rather than solving security problems as operational reactions to independent events. This language-oriented approach to security problem formulation also helps the

OCA implementation community to better index and share security-prevention knowledge in formalized linguistic patterns.

Cybersecurity knowledge accumulation, searching, and presentation

Following the doctrine that security problems should be formalized as linguistic patterns. OCA-NS-SEC is the namespace to store solutions to security problems. Each solution pattern should be encoded as a formalized language that could represent and execute security-assurance actions. The accumulation and presentation of cybersecurity knowledge should be carried out by a knowledge engine based on OCA-NS-SEC that serves as an encyclopedia of precisely defined cybersecurity terms. As new security knowledge gets accumulated, a large number of solution patterns will grow accordingly. To manage the continuously growing knowledge base, popular software platforms such as Mediawiki can be used to store these cybersecurity terms. Using Mediawiki as the basis for cybersecurity knowledge management has many advantages. First, Mediawiki is open source, which has a wide range of software extensions. Second, Mediawiki is a web-based information dissemination platform, which allows an end-to-end, from content-submission, to content-publication, full content lifecycle workflow. Storing and sharing cybersecurity knowledge content in Mediawiki-based data format could significantly boost the transparency and up-to-date synchronization of cybersecurity knowledge. A publicly accessible OCA-compliant Cybersecurity website powered by Mediawiki could also immediately serve as a knowledge disseminate channel. Therefore, the security knowledge content designed to educate the public should be based on OCA-NS-SEC and eventually become learning material to appear in OCA-NS-EM.

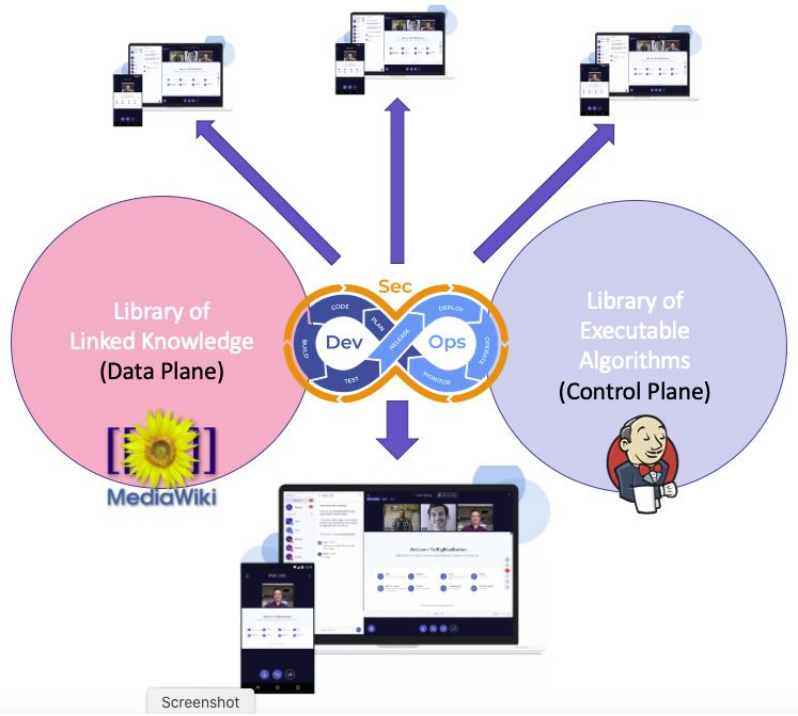
A key feature of MediaWiki is its extensibility. To make cybersecurity knowledge readily accessible to a wide range of scenarios, high performance search and data visualization must be integrated with MediaWiki. So far, ElasticSearch and Kibana are customizable search and data visualization tools that have already been integrated with MediaWiki. Configuring MediaWiki with highly flexible search engine and visualization technologies is a necessary knowledge infrastructure for the whole cybersecurity knowledge sharing community. These indexing, searching, and interactive exploration features of MediaWiki and ElasticSearch can be applied to manage all content in OCA-NS.

A dedicated workflow executor that utilizes localized, computable knowledge

While MediaWiki works as a knowledge storage and presentation engine, without an autonomous executing agent that acts on this stored knowledge, the stored content can only be passively retrieved. Knowledge about Cybersecurity cannot only be viewed and used passively. Knowledge about security needs to be transformed into actionable data. An open source tool, Jenkins, is designed to perform many security-sensitive process automation tasks. Knowing that Jenkins is also the de facto tool designed to automate the activities for CICD/DevSecOps, the way Jenkins is being deployed to critical cybersecurity infrastructures should already have a repertoire of best industry practices. Some of the best practices have been published on the web, such as [33,34].

Jenkins is also intended to be used with MediaWiki, so that instructions on how to utilize Cybersecurity protection and how to install software/hardware, or employ protective measures can be found in MediaWiki.

The content of MediaWiki should adopt standard templates that categorize Jenkins related web pages to have integrative features. Streamlining the connection between Jenkins and MediaWiki is an important engineering task for OCA-compliance. Ultimately, all data flows that come onto users' endpoint devices (personal smartphone, laptop, workstation) should all go through a proxy that adopts DevSecOps procedures to pre-emptively protect users' cognitive bandwidth. Users can have full local sovereignty to decide what and how information can come through and how they are presented or tracked in users' local knowledge repository.



To ensure that all users can protect themselves by practicing OCA-compliant protection procedures, the above-mentioned MediaWiki+Jenkins infrastructure is designed to be owned and operated by individual persons. By allowing anyone to own and operate their own knowledge repository and automated cybersecurity execution agent, this allows everyone to have symmetrical rights to protection, that adheres to the Principle of Information Symmetry.

WebRTC and Browser-based Information Presentation

Due to the maturity of Browser-based technologies, every web page can be organized as a self-sufficient computing platform by itself. Supported by industry standards, such as WebRTC, WebAssembly, and HTML-5, deploying functional features to networked devices is becoming more convenient and the costs associated with developing the solutions is also reduced. It also lowers the entry barrier for people who want to adopt OCA-compliance. Therefore, WebRTC and browser-based technologies will be the first choice when new client-side technologies must be developed.

Boundary Conditions: Expected Challenges

Omnia Cybersecurity Architecture (OCA) is a technical specification that obeys the Principle of Information Symmetry. The benefit of leveraging data, people, processes, and tools developed under the principle of sharing and equality, reduces the competitiveness in proprietary solutions. Clearly, there should be commercial incentives to help further develop cybersecurity solutions. OCA is designed to accommodate either commercial or publicly available solutions, as long as the minimal requirements of information symmetry is obeyed. Cybersecurity is not an isolated industry, it is an emerging transdisciplinary field that is already being considered as a strategic part of national security programs. More importantly, it is shaping the way we produce and create new solutions in both physical and cyberspaces. The challenge is not about whether or when cyberattacks would take place, the challenge is to establish a sustainable operation principle that would enable continuous flourishing of new ICT capabilities and solutions, while maintaining a tolerance level that can cope with unavoidable damages. By adhering to the Principle of Information Symmetry, even certain damages are too severe for one organization to bear, its operational experience could benefit future organizations to avoid future damages, therefore reducing the ongoing impact of cybersecurity skirmishes.

To avoid reinventing the wheels, OCA incorporates existing best practices in the ITC industry, such as CICD[18] and DevSecOps[19]. In addition to known industry practices, OCA also emcompasses a developmental protocol to define public Application Programming Interfaces (API) for automatic negotiation and coordination mechanisms across organizational boundaries. The developmental protocol and public API would expedite symmetric information sharing and should also work across political borders, since cyberspaces can easily permeate across physical jurisdiction zones.

Political Risks: The Cyber-warfare in Data Collection and Data Access

The data management agencies, or agencies that have the ability to process security-sensitive data will have a profound, asymmetric advantage over agencies and persons that do not have the ability to process large personnel movement data. This opens

[18] CICD stands for Continuous Integration and Continuous Delivery/Deployment.
[19] DevSecOps is an extension of DevOps, which means Development + Security + Operations.

up a new area of data governance that were not inherently designed into current government administrative processes. Therefore, introducing new capabilities and new policies at a speed of data collection becomes the first question of organizational sovereignty. Without localized ability to process and analyze the consequence of location sensitive data, the security of that localized region can be intermittently transferred through undetectable data pipelines, and eventually expose critical information about the cyberspace system under protection.

Data security issues are not limited to one kind of data, but data collection and access rights in general. However, data collection and access management is not just a technical topic, it is also a highly political topic. The rights to collect and access data are often embedded into government policies, local politics, and the enabling technical architectures. These three kinds of things may not be consistent, and may never be synchronized in time. One may imagine all three things mentioned above, government policies, local politics, and technical architectures are three loosely interacting Kuhn Cycles, that each triggers the others to go into different stages of model drift, model crisis, model revolution, and paradigm change modes. It is hard to envision that either government policy refinement or local politics can be systematically accelerated, other than using a CICD/DevSecOps-like procedure to inform a significant portion of the participating crowd. Therefore, government agencies, relevant political actors, and technology suppliers, should all be equipped with a transparent and customizable communication mechanism to receive and propagate information in an actionable and traceable format, so that the game-theoretic political reasoning dynamics can be captured in a public, OCA-compliant data platform. This generalizable reasoning mechanism should and could only start with the Principle of Information Symmetry. Translated into a technical trust-model, one can consider that Self-Sovereign Identification and a unifying Name-space management practice could keep many parties and cyberspace actors accountable for their actions, therefore obtaining systematic security protection through being OCA-compliant.

Voice in the Wilderness: The nature of Cyber-Attacks

Due to the secretive nature of cyber-attacks, it is possible to systematically introduce damages to a system without revealing any noticeable signs. It would be necessary to mention that societal crises often arise when the technological advancements creates

incommensurability problems in the general public. A significant amount of social tension and systematic damage are done by the general public who are not aware of their collective actions could result in dire situations. Using Botnet[20] to launch cyberattacks is a common practice of hackers exploiting information asymmetry. Most of the people who own computers that run "Botnet" software are simply unaware of their devices' clandestine activities. Unbeknownst to the computer owners, their machines are simply infected by malicious software, and can only be intentionally stopped and removed when the owners become aware that their machines are being used for cyberattacks. Generally speaking, information asymmetry can be exploited in many ways, and it could only be resolved at the root by enabling periodic, yet timely update of cybersecurity knowledge. People who own connected computing devices should regularly run "trust-worthy" device cleansing software to examine their own devices. However, as of year 2020, most of these device cleansing software are created by commercial security service providers, it is difficult to determine the degree of trust-worthiness of these device cleaning software.

A Scenario of Cross-Domain Data Security Breach

Physical devices, large social organizations, financial accounts can be controlled by some unauthorized parties undetected for a long time, all before a major attack strikes. Using Covid-19 epidemic as an example, security holes may be wide open, yet no one in the authoritative system has a cure, so that the whole system can be vulnerable to attacks to a wide range of eventual systematic attacks. For instance, due to the lock-down policies of Covid-19 Epidemic, many governments started to require citizens to expose their travel history information on their personal cell phones. This information exposure to public security agencies may or may not have been managed in a secure manner. The exposure of real-time personal location data is not only an intrusion of privacy, but also a major security concern for the society. Collecting personal movement data at a massive scale, while not having public oversight on this large amount of personalized data is a major security risk. Without a technical architecture that programmatically recognizes the sovereign control policies of personalized data, no one knows how many parties might have access to the human movement data on a large scale.

[20] Botnet is a way to use malicious software to control distributed devices owned by innocent users to launch attacks in cyberspace. For more information, please see Wikipedia: https://en.wikipedia.org/wiki/Botnet

Conclusion:

To attain a desirable level of cybersecurity requires a principled approach, the Principle of Information Symmetry. This principle can penetrate security-breach crises across all spacetime contexts, while it is succinct enough to enable speedy recognition. The principle can remind us of the complementary nature of the safety and liveness conditions of a system, and allow automatic, self-aware procedures to check and inform relevant authorities ***continuously***. The ICT industry has been working on this problem for a long time, and methodologies such as CICD/DevSecOps, and tools such as K-Framework, Jenkins, MediaWiki, Istio (Service Mesh implementation), ElasticSearch/Kibana, and many others have been incorporated in various toolchains to galvanize cybersecurity. It is the purpose of this document to entail a rapidly responsive, open-sourced, language-oriented, real-time data driven, self-sovereign security architecture, so that the security governance capabilities could be made available to anyone, anywhere.

A self-governance model that is trust-worthy to all

This document provides a high level overview to explain how all these methodologies and tools can be put together to protect an individual or an organization. It clearly needs the proper support and participation of stakeholders. The Principle of Information Symmetry is not just a philosophical idea, it also embeds the technical meaning that defines the compositional properties of a system, so that it assigns the rights and responsibilities in ways that help a living system to attain security awareness with a technically grounded infrastructure. It is evident that no one person, even a large country can afford to synchronously update its cybersecurity infrastructure to all its relevant stakeholders at all times. It is also impossible for a large number of users to know the working details of any technically sound security model. However, by presenting an open sourced approach to both the governing model, as well as publicly exchanged operational data, it provides the working examples to allow people to choose from which governance model is more suitable for them. The OCA-compliant platforms for executing these governance models are designed in ways to be interoperable, so that governance models can be shared and tested across communities that follow the Principle of Information Symmetry through OCA-compliance.

The Principle of Information Symmetry is Apolitical

It is also necessary to point out, the Principle of Information Symmetry is a neutral term by definition. It is the intellectual and cognitive foundation for scientific exploration, mathematical computation, legal interpretation, and logical induction and reduction. It doesn't challenge any existing ***rational*** belief systems, it is simply a statement of fact that all decision or cognitive processes are about detecting the conditions or boundaries of information symmetries. Once certain detectable differences can be found, information symmetry is broken. When working across different mathematical or physical abstractions, the Principle still can work in surprisingly fundamental ways. The Principle of Information Symmetry is not a political statement, it is a technical term that defines the recognition that information comes from the awareness of differences over artificially defined namespaces and the physical spacetime. When working in the context of cybersecurity, it is information symmetries that define the boundaries of sameness, where it gives people a basis to compare, to become aware of change, so that decisions can be made in different human contexts. By operationalizing cybersecurity infrastructure around the Principle of Information Symmetry, it avoids policies or decisions to be made only based on anecdotal evidence. It would utilize operational historical data, as well as linguistic logic, to decouple security policies from social engineering or emotional/media maneuver. So that even bad policy decisions are made, it becomes transparently trackable that under what operational context certain decisions are made, and why the decision was considered "bad" on a technical ground. OCA is designed to be a public standard, it tries to contain enough technical and operational mechanisms that are relevant to cybersecurity management. Its actual implementation, whether good or bad, is intended to be exposed and adjusted according to the very nature of its architectural principle, the Principle of Information Symmetry.

Epilogue:

In the science of secrecy, often known as the art of cryptography, is an iterative game of keeping symmetry and symmetry breaking. Through the process of keeping every alternative possible, the possibility space delivers a degree of freedom to decision makers. It is the decision-maker's awareness of available possibilities, that guides the evolutionary paths of future fates. Without confusing or overwhelming users with technical details, a generalizable cybersecurity management practice, must present the broadest possible options to its stakeholders, and even guide them with occasional convenience to utilize the knowledge of symmetry to compress system complexity. Going back to the Venn diagram of system correctness, the process of achieving safety and liveness is iterative, it gives and takes some areas of opportunities continuously. It is the act of exerting checks and balances that help the system to stay true across its entire lifecycle. This simple, finite invariance, allows OCA to present a finite, self-determined, self-sovereign model of Cybersecurity. It is this time-based, iterative model of security model evolution, that provides an abundant space for future possibilities.

To help cybersecurity experts to better associate the Principle of Information Symmetry to their jobs on an operational level, the five categories of symmetry is presented below:

1. **Natural or Structural Symmetry**: The general property of invariance. Without any prior knowledge and technological infrastructure, all things are assumed to be equal and random, this is the zeroth order symmetry, which can be used as the basis for measuring complexity, often known as entropy. The commonly known natural symmetries are time, space, energy, and electric charge conservation laws. These ideas of symmetry also relate to the mathematical notion of naturality[35, 36].
2. **Data Content Symmetry**: For required, basic survival data, such as medical information, quality of food, water, shelter, etc. are life supporting data that must be provided to all members of the society. Another technical term that is almost synonymous to data content symmetry is data immutability. It means that public data assets should be made consistently accessible and tamper-proof.

3. **Functional Symmetry**: Algorithms can only function properly when data structures are exposed transparently. Therefore, data indexing, data search, data format conversion schema, data visualization software components, and DevSecOps related authentication and authorization token data structures, must be revealed to the public. One may also consider this is the symmetry in algorithm space. This symmetry also allows zero knowledge proof to be applied to data content that must be kept privately while allowing publicly known algorithms to check its validity.
4. **Infrastructure Symmetry**: For certain aspects of publicly funded ICT capabilities, such as basic communication bandwidth, data processing units (CPU, GPU, TPU), their availability should be presented in public and in non-protective data formats. Overtime, publicly available data processing resources should also be publicized in ways that serve anyone who wants to use them. Conversely, certain privacy sensitive data, such as email addresses, IP Addresses, Internet DNS traffic data, as well as Self-Sovereign Identity, should be protected using privacy protection mechanisms in the public infrastructure as much as possible. This symmetry makes a functional system trust-worthy.
5. **Knowledge Symmetry**: OCA-compliance means the provision of free, and open educational content, to instruct all participants to learn and use the above mentioned symmetries. Most essentially, explain the Principle of Information Symmetry in operationally and culturally meaningful terms. The goal is to maintain equality in the ownership structure of information interpretation, equality in terms of equal interpretive powers, while allowing owners' freewill judgements based on their localized/private knowledge.

We may compress all of security concerns in one sentence:

Governing cybersecurity through the Principle of Information Symmetry.

The principle is about protecting the inherent differences between people and organizations. Everyone should have their distinctive features and make decisions in unique and idiosyncratic ways. But the methods and tools to determine the justification should be designed indifferently, so that some regularities[37, 38] would be accumulated to help future versions of this society to better cope with the social evolutionary stages covering from model crisis to paradigm shifts as stated in Khun Cycle. OCA is designed to

enable and govern interactions between different parties in cyberspaces. It should work to protect privacy and property rights while ensuring public safety. When private interest and public interests have direct conflict, an equitable procedure, executed by transparently defined laws can be used to break the contention. This is the Symmetry in Public Knowledge.

About the Authors

Ben Koo

Hsueh-Yung Benjamin Koo, is an Associate Professor at Tsinghua University, where he founded the practice of Extreme Learning Process (XLP) for designing and operating Scalable Learning Organizations. His research areas range from the theory of systems architecting, smart city development, and the technology of governance. He currently works on the project of creating Tsinghua South East Asia Center, located in Bali, Indonesia. The project is about utilizing ICT infrastructures to enable city planning and development projects and using these projects to provide an authentic learning experience to participants around the world. Prof. Koo holds a Doctoral Degree in Engineering Systems, and a Master Degree on System Design and Management, both from MIT. He also earned a Bachelor Degree in Mechanical Engineering from the University of Minnesota.

Sue Kamal

Sue Kamal is an Award Winning Global Entrepreneur and International Business Developer with a strong network foothold around the globe. She holds a Certificate and Degree of Law (LLB Honours) from IIUM. She co-founded SMC Emirates, a business consultancy and advisory firm in Dubai, UAE and set-up another two business entities in Malaysia. Sue possesses a vast experience in international trade and investment which also include having expertise in business development, branding, corporate communication as well as management, gaining her the Entreprenologist Accreditation, the highest accreditation for an entrepreneur by WAVE USA. Her hands on experience has been leveraged by the Malaysian Government for its National Entrepreneurship program, including upscaling businesses for digital transformation and adoption. Her active work and contribution in the Gulf region has gained recognition by local leadership as well as Members of the highest authority. Her involvement in the economic and infrastructure development effort for the Sultanate of Oman is pivotal, leading her to recently being appointed at the Government level for Malaysia - Qatar Business Council upon strengthening the bilateral trade between the State of Qatar and Malaysia. Sue is very good at naming things, the name Omnia in OCA, was assigned by Sue.

Acknowledgement

Prof. Gautam Dasgupta organized a large number of experts to provide feedback to refine this document. Prof. Ray Daugherty provided very insightful guidance and engaging discussions over many months. Prof. Probal Dasgupta, whose ideas on how language, especially natural languages should be included as a source for computable knowledge management, is a major highlight of our team-based discussion. Dr. Kundu Suorav also provided many penetrating technical advice in refining this document. Prof. Veikko Karenen offered technical references to Topological Entropy and other mathematical constructs that led to discussions about the formulation of generalizable security metrics. This idea advanced the OCA governance model significantly. He also provided corrections to the history of GUN-Linux and the Open Source Code/ Free Software Movement.

Tong Ziquan worked on refining the overall document and presented many stimulating questions that shaped the direction of this article. Twain Liu's ground breaking thoughts on modeling and human cognitive is a major inspiration to the first author. John Havens provided guidance to explore and study the application of self-sovereign identity technologies for cybersecurity governance. The first author also wants to thank Dr. Konstantinos Karachalios for his long time friendship and thoughtful provocations in the framing of this cybersecurity governance from a technology standards' viewpoint.

References

1. Laura Bell, Michael Brunton-Spall, Rich Smith, and Jim Bird, Agile Application Security: Enabling Security in a Continuous Delivery Pipeline, O'reilly Media, 2017

2. Hsueh-Yung Benjamin Koo, A Meta-Language for Systems Architecting, MIT Ph.D. Thesis, 2005

3. Susan Owicki, Leslie Lamport, Proving Liveness Properties of Concurrent Programs, ACM Transaction on Programming Languages and Systems, Vol. 4, Np.3, July 1982, Pages 455-495

4. DevOps.com, DevOps: The Driving Force of the Industry, last accessed: July 10, 2020

5. Leslie Lamport, Robert Shostak, Marshall Pease, The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems, July 1982, pp. 382-401

6. Leslie Lamport, Time, Clocks, and the Ordering of Events in a Distributed System, Communications of the ACM, July 1978, Volume 21, Number 7

7. GNU Website, What is Copyleft? URL: https://gnu.org/licenses/copyleft.html, Last accessed: July 24, 2020

8. Lawrence Lessig, Code and Other Laws in Cyberspace, Basic Books, 1999

9. Robert G. Eccles, Michael P. Krzus, with Sydney Ribot, The Integrative Reporting Movement: Meaning, Momentum, Motives, and Materiality, Wiley, 2015

10. Editors: John Hughes et al., Profiles of the OASIS Security Assertion Markup Language (SAML) V2.0, in PDF form, published March 15, 2005, last accessed July 27, 2020

11. B. Koo, M. Poonawala, W. Tsai, E. Qiu, Network Publishing Paradigm: A Web Authoring and Publishing Methodology for Internet Commerce, electronic publication, IICS-MN, 1996.

12. Koo, et al., Extreme Learning Process(XLP): the Owners' Manual, in PDF form, last accessed: July 10, 2020

13. Thomas Khun, The Structure of Scientific Revolutions, University of Chicago Press, 1970

14. Don Tapscott, Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, Portfolio, Reprint Edition 2018

15. Ahmed Afif Monrat; Olov Schelen; Karl Anderson, A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities, IEEE Access, published August 19, 2019

16. Jane Gleeson-White, Double Entry: How the Merchants of Venice Created Modern Finance, W. W. Norton & Company, 2012

17. Satoshi Nakamoto, Bitcoin: a Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, last accessed: July 24, 2020

18. Mark Robinson, DevSecOps, a Complete Guide to What, Why, and How. https://www.plutora.com/blog/devsecops-guide, last accessed July 10, 2020

19. XebiaLabs, DevSecOps: The Missing Link in Delivering on the Promise of Business Velocity, published 2018, last accessed July 10, 2020

20. John Rawls, A Theory of Justice, Harvard University Press, Revised Edition, published 1999

21. Hristo Koshutanski; Mihaela Ion; Luigi Telesca, Distributed Identity Management Model for Digital Ecosystems, The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), IEEE, 2007

22. Geoff Goodell; Tomaso Aste, A Decentralized Digital Identity Architecture, Front. Blockchain, Published November 05, 2019, last accessed July 20, 2020

23. Timothy Ruff, The Three Models of Digital Identity Relationships, How self-sovereign identity (SSI) is different, and why it's better, Evernym, published on Medium, last accessed: July 20, 2020

24. Gabriel René; Dan Mapes, The Spatial Web: How Web 3.0 Will Connect Humans, Machines, and AI to Transform the World, published August 26, 2019

25. Philip Windley, Digital Identity, O'Reilly Media, 2008

26. Phil Windley 2018, Multi-Source and Self-Sovereign Identity, published 2018, last accessed July 11, 2020

27. Christopher Allen, The Path to Self-Sovereign Identity, Published 2016, last accessed July 21, 2020

28. Jemielniak, Dariusz, *Common Knowledge? An Ethnography of Wikipedia*, Stanford University Press, 2014, ISBN 978-0-8047-8944-8

29. Gartner, Integrating Security into the DevSecOps Toolchain, published 2019, last accessed July 10, 2020

30. Cuelogic Technologies, Istio Service Mesh: The Step by Step Guide, published 2019, last accessed July 11, 2020

31. Eric Rescorla, SSL and TLS: Building and Designing Security Systems, Addison Wesley, 2000

32. Xiaohong Chen, Grigori Rosu, A Language-Independent Program VerificationFramework, ISoLA'18, Springer, pp 92-102. 2018

33. James Lee, How Important is DevOps for Facebook and AWS?, Level Up Website, https://www.level-up.one/important-devops-fb-aws/, Nov 2, 2018, last accessed July 14, 2020

34. Veritis, Transitioning from DevOps to DevSecOps: integrating "Security as Code" culture to DevOps, last accessed July 10, 2020

35. Emmy Noether, Invariant Variation Problems, M. A. Tavel's English translation of Noether's Theorems (1918), reproduced by Frank Y. Wang.

36. Samuel Eilenberg, Saunders MacLane, General Theory of Natural Equivalences, Transactions of the American Mathematical Society Vol. 58, No. 2 (Sep., 1945), pp. 231-294

37. Leslie Valiant, Probably Approximately Correct, Nature's Algorithms for Learning and Prospering in a Complex World, Basic Books; 1st edition, June 4, 2013

38. L. G. Valiant, The Theory of the Learnable, Communications of the ACM, November 1984 Volume 27 Number 11