**Omnia Cybersecurity Architecture**

horizontal line

# An Inclusive infrastructure for Self-Sovereign Citizen-Centric Cyberspace

# 

# 

# 

# 

# 

# 

### Author: Ben Koo, Sue Kamal

# 

# 

# 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 exchange 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 diagnose cybersecurity challenges at a common root, Omnia Cybersecurity Architecture (OCA) detects cyberspace asymmetries in terms of the changing speeds of data distribution. Using the case of high-frequency trades as a revealing 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. Intention 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 evolution as a creative common. It is the transparency and inclusivity that distinguishes OCA from other security architectures that has inherent commercial and political interests. 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.

# Introduction to Omnia Cybersecurity Architecture

## Cybersecurity Threats in the Contemporary Context

Under the ongoing global movement restrictions caused by Covid-19, the social functions of Information and Communication Technologies (ICT) started to elevate from supportive roles in the past into the current leading role. It would be fair to state that 2020 is the year that the whole human race is being grounded in physical spaces to ponder about the future in our collective cyberspace. One may argue that information asymmetry about the epidemic nature of Covid-19 was a major cause of this ongoing 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[[1]](#footnote-0) have influenced strategic political outcomes in several nations. By now, it is generally recognized that new ICT capabilities can induce asymmetric advantages in political campaigns, economic development programs, and can transform 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, autonomous vehicles and machine learning algorithms. Each one of these new capabilities has the potential to fundamentally shift the business paradigms and to change social norms of their respective application domains. The combined effects of these new capabilities are even more impactful to the global society. 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 the overarching framework to diagnose and tackle existing and emerging threats with one unifying security protection principle: sustain system safety via the maintenance of information symmetry.

## The Goal: Maintain Information Symmetry through ICT

Given the social impact and potential benefits of ICT, national governments recognized the need to regulate cyberspaces. The dynamic and technical nature of ICT, which defines the operational properties of cyberspaces, continuously challenges the very notion of property rights in cyberspace must be continuously updated according to the new capabilities offered by ubiquitous ICT infrastructures. However, the deployment speed of new technologies can easily outpace the speed of regulatory reactions. In principle, to maintain order and justice in cyberspace, all stakeholders must have symmetric access to information. For critical public infrastructures, policy makers and policy making procedures should adopt ITC 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:

Incorporate cybersecurity policy compliance checks across all stages of public technology development and deployment projects by exercising global best practices available in ICT industry, using the most inclusive infrastructure, data formats, and human interfaces to ensure transparency and scalability.

## Cybersecurity Objectives in a Measurable Framework

An overarching framework that can orchestrate people, process, and tools to maintain information symmetry should be encoded in an implementation oriented architecture. This document presents Omnia Cybersecurity Architecture (OCA) to define a conceptual boundary to operationalize the abstract goal maintaining information symmetry. Paraphrasing ISO/IEC/IEEE 42010’s definition of technical architecture, OCA prescribes the fundamental rules to organize key stakeholders, process structures, and enabling technologies that enable the design and evolution of cybersecurity governance. To avoid reinventing the wheels, OCA incorporates existing best practices in the ITC industry, such as CICD[[2]](#footnote-1) and DevSecOps[[3]](#footnote-2). 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 national borders, since cyberspaces can easily permeate across physical national jurisdiction zones.

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

1. Embed cybersecurity compliance verification procedures into product/service development and operational activities using programming interfaces available to the public
2. For products and services relates to public safety, technology suppliers are required to continuously publish safety compliance verification data to the public via the above-mentioned programming interface
3. A public data log (historical data) that represents public cyberspace activities should be recorded using “real-time”, and immutable databases, often relates to the notion of blockchain. This data log can be witnessed by the public, and therefore hold relevant participants accountable for their activities in public[[4]](#footnote-3) spaces.
4. Cybersecurity compliance data should be presentable in popularly accessible browser software and mobile computing devices, so that the data could be conveniently viewed and analyzed using data visualization and data mining techniques by average citizens
5. Dedicate developmental resources to create OCA-compliant educational material for popular and publicly-funded Cyberspace technology development projects. The investment in OCA-compliant educational content development could ensure the ongoing adoption of cybersecurity practices based on the principle of information symmetry. This OCA-compliant educational material 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.

## OCA Implementation Outcomes and Instrumentation

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 different resources dedicated to preserving their desirable level of cyberspace safety. To attain self-sovereign cybersecurity practice, there is a minimal set of requirements that must be fulfilled. OCA defines these requirements as follows:

1. An agency or a dedicated person (agent) in the organization of interest that would be responsible for the cybersecurity compliance verification procedures. This agency or agent should be able to operate automated compliance verification machineries, so that many of the cybersecurity verification procedures can be scaled up to serve the general public or the organization’s intended customers. The agency or agent should also have the authority to issue and modify the operational procedures of the above-mentioned machinery.
2. Subscription to the Principle of Information Symmetry: to implement any level of cybersecurity protection in an organizational level, certain operational data will naturally be shared amongst multiple stakeholders. Knowing that any form of data sharing could reveal privacy and therefore have security consequences, the best one can do is to ensure that data is shared based on the Principle of Information Symmetry. This principle is derived from ideas originally articulated by the Founder of Free Software Foundation, and creator of GNU-Linux, Richard Stallman[[5]](#footnote-4), but the short version is that all stakeholders will be given the equitable rights to data assets comparable to their contribution rights or their organizational responsibilities. The nature of cyberspace allows equitable rights and organizational responsibilities to be explicitly defined in executable code. The Principle of Information Symmetry also requires that this explicit definition of rights and responsibilities be revealed to all participation members transparently. Information security should only be asserted based on this minimalistic assumption of data sharing and rights allocation, and should be adopted as a principle for public cyberspace security systems.
3. The cybersecurity agency of the organization of interest should subscribe to, or establish an original immutable, realtime data service as a public event recording ledger (inspired by blockchain technology). This data service provides a public registry of temporally ordered events, similar to the postal time-stamped filing of provisional patents. This immutable data service will create a verifiable link between physical space and cyberspace through the time dimension. This temporal bridge can be used to infer causal relations and compute correlations across the boundaries of all physical and cyberspaces, providing a referential data plane to analyze and detect the pulse of impending security threats synchronized in real time.
4. The Cybersecurity Agency should have a publishing workflow that continuously refines and updates a single User-Machine Interaction interface. This user-machine interface will enable its stakeholders to receive continuously updated security threats on the most convenient devices, such as their personal cell phones or laptops. This publishing workflow needs to be mindful of the cognitive load of its users, so that the informed end users would receive intuitive, timely, but not overwhelmingly frequent bombardment of alert signals. The requirement of this publishing workflow is to deliver actionable signals to end users of cybersecurity related infrastructure at the appropriate points in spacetime, so that these signals could help minimize or avert expected damages.
5. A Cybersecurity research and educational content development team. This team will develop educational material to inform casual users of public infrastructures, and train engineers and operational staff members who are responsible for developing or maintaining security critical public 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.

## A Meta Process of Governance

The process of engaging an existing organization or national entity to practice sustainable cybersecurity protection practices should also be compliant with the Principle of Information Symmetry.

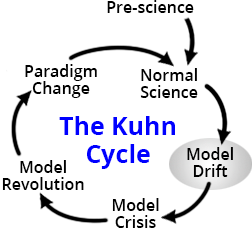
### Advancements in ICT introduces unprecedented Governance Methods

Attain Security through effective name management

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. A recent trend in using Botnet[[6]](#footnote-5) to launch cyberattacks is one more example of hackers exploiting information asymmetry. Most of the people who own machines that run Botnet software are simply unaware of their devices’ actions. Their machines are simply infected by malicious software, and can only be stopped and removed when the owners become aware that their machines are being used for cyberattacks. Generally speaking, incommensurability can be exploited in many ways, and it could only be resolved at the root by enabling periodic, yet timely update of cybersecurity knowledge.

### Scientifically Exploit Information Asymmetry

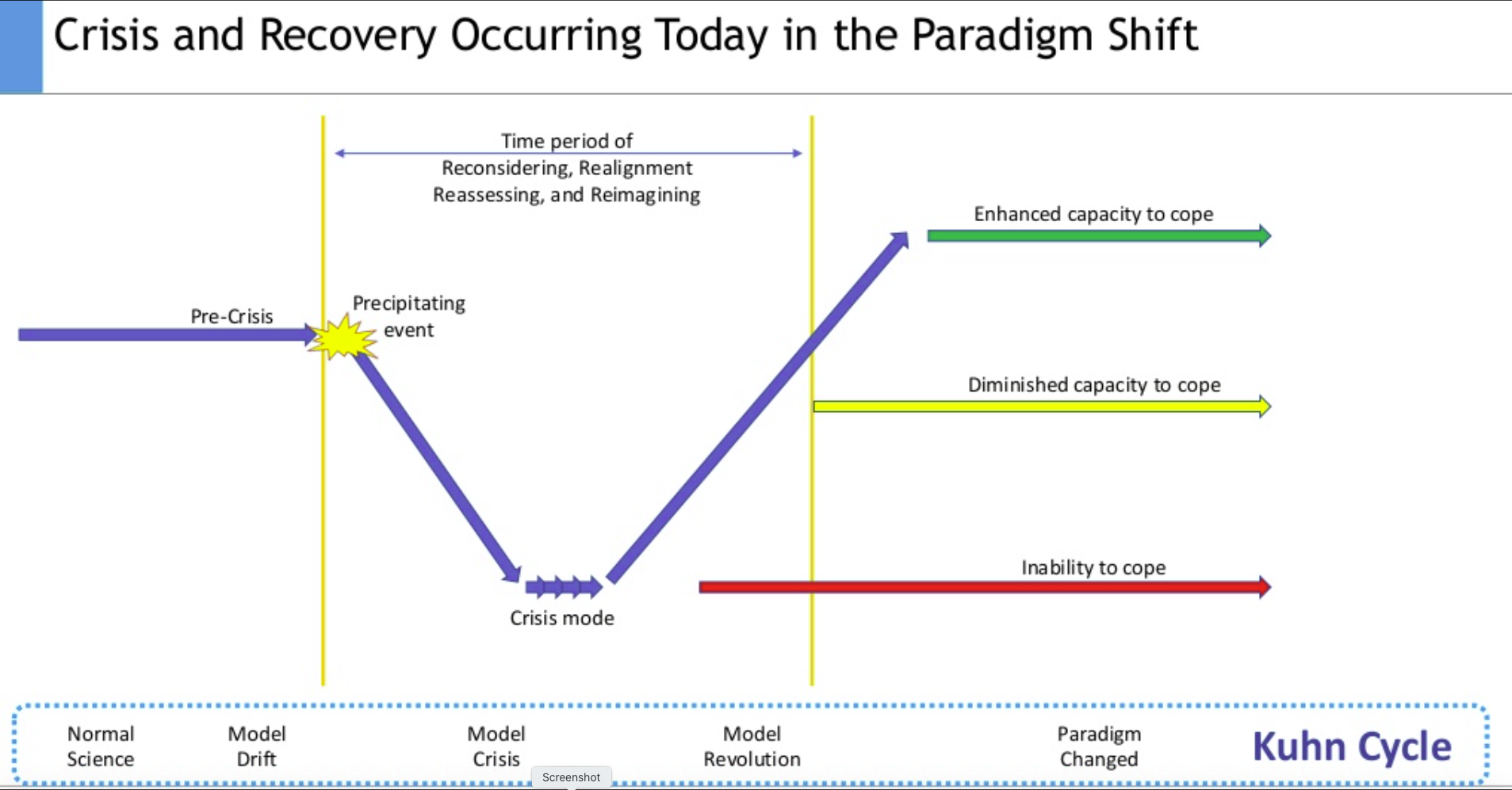
Thomas Khun, author of the book, the Structure of Scientific Revolution, the cyclic process of scientific discovery naturally the systematic conflict caused by incommensurability. The following diagram shows the self-correcting cycle presented by Khun.



In the context of cybersecurity protection strategy, the issue is not whether the society will correct itself, it is when and how fast the correction can take place. Clearly, the faster the cycle could be turned, the less damage incommensurability could exert on the system. 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.

### Models of Capability Maturity and Incommensurability

In the world of cybersecurity, a reliable cybersecurity patch, often requires the software vendor, especially the operating system supplier to fix the security problem at the source code level. When more critical infrastructures are being controlled by software, this means that all critical infrastructure projects must be able to rapidly deliver security patches. Otherwise, while waiting for security patches, critical infrastructures would be shut down for a long time. The following diagram drawn by Software Architect/Systems Engineer Mark Reynolds, presents the opportunities and danger zones in different colors. When reaction time is longer than the cybersecurity team’s ability to present a new solution, system failures occur.



Based on the Principle of Information Symmetry, OCA deals with all crises and recovery opportunities in a uniform fashion. Historical records of previous cybersecurity attacks and solutions of other similar projects can be reused for future projects. To incentivize data and solution sharing, Open Source styled development practice is heavily encouraged. In other words, OCA considers Cybersecurity Solutions as a form of public goods, it should be shared and made available to all.

### Language as a container for Information Symmetry Management

Another pragmatic angle of the Cybersecurity Recovery process model is the speed of resolving a specific technical problem. To expedite the recovery speed throughout the entire product lifecycle, the ICT industry has been practicing a product-specific security enhancement process model known as DevSecOps and CICD. The successful implementation of DevSecOps and CICD requires a significant amount of automation and disciplined software engineering practices. These will be discussed in the next section.

## Required Resources and Enabling Process Models

To execute and maintain OCA-based cybersecurity practices, one would need the following infrastructural components:

### People:

#### 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, 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 SSI” [[Web](http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html) 2016].

#### Cybersecurity Administration Staff:

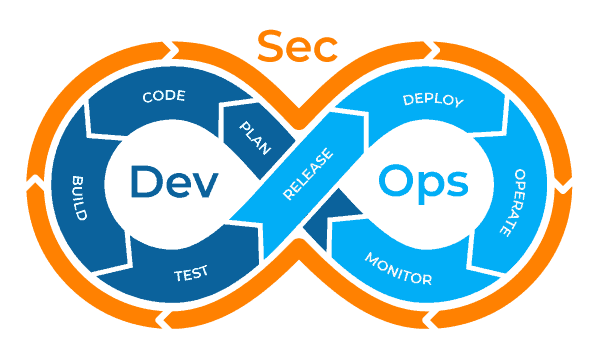
The operation of OCA-compilant critical infrastructure would require multiple dedicated professional cybersecurity staff members to plan, execute, and maintain the health conditions of infrastructure cybersecurity. The skill requirement is that the composition of these professional staff must cover the 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 Standards

The cybersecurity industry is still at its infancy. Many new application areas and use cases are still to be invented. The OCA-compilant process model will encourage all stakeholders to actively participate in the shaping of industrial standards. Cross Disiplinary 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 area of law enforcement, of universal basic rights and ethical concerns are particularly ripe for new industry standards, because many of the law enforcement policies can be directly implemented using cybersecurity governance technologies.

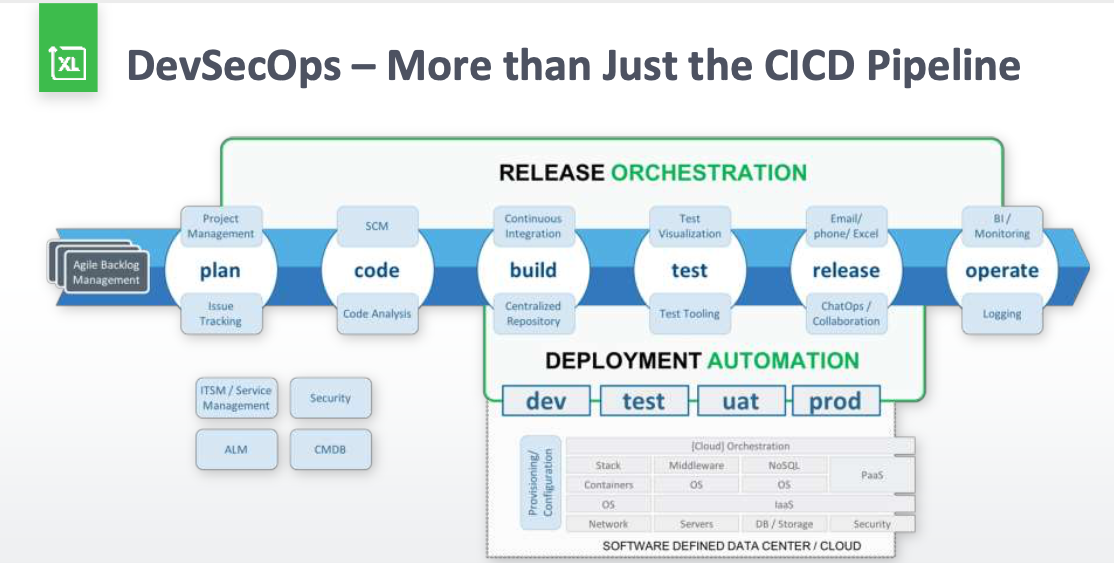
### Process:

The latest well-known Cybersecurity Process Model is called: CICD/DevSecOps. On the highest level, DevSecOps can be understood as an extension to the infamous DevOps Logo shown as follows:



This logo reveals that DevOps is an iterative cycle of eight distinctive service/product planning and deployment subprocesses, while security wraps around all of these eight subprocesses. It simply means that security verification practices must be inserted into all stages of development and operations activities. OCA subscribes to DevSecOps’s “security first awareness” philosophy.

However, there are two more layers of security concerns that go beyond the scope of DevSecOps. First, to expedite the Development to Operations cycle, inserting security checks and verification policies can easily slow down the product release cycle time. Second, most DevOps development practices often adopt another layer of process model, often called CICD, a.k.a. Continuous Integration and Continuous Delivery/Deployment. This additional layer of process model accelerates product release cycles using a collection of process automation tools. This additional tooling efforts actually elevates the technical barrier to entry, and also increases the initial set up time to product development. However, once it is set up, the overall development to operation process would be much more streamlined. A typical DevSecOps enhanced CICD workflow can be found in the diagram created by XebiaLab’s as shown below.



#### A generalized process for transforming non-ICT Intensive Industries

As the diagram above reveals, modern ICT-based product and service deployment is orchestrated using highly automated toolchain. This comprehensive set of toolchain actually could also be applied to a wide range of non-ICT centric product development and deployment activities. In fact, manufacturing and energy sectors are starting to adopt CICD and DevOps practices. The key point is that once a full-blown CICD/DevSecOps tool chain is built, the entire platform can be modularly applied to many other similar industries.

#### Use OCA-compliant Educational Process to raise Security Awareness

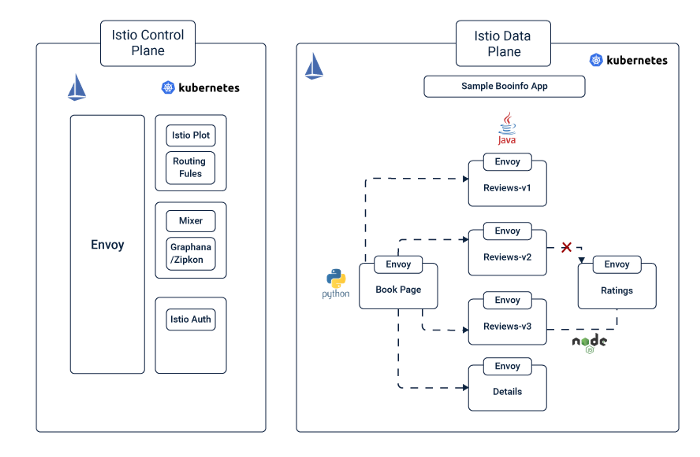
Up to the time of this writing, DevSecOps and CICD is still only being practiced in rather elite software development communities. However, in the ever accelerated Cyberspace arena, time is not only money, the ability to procure the best practice also significantly advances the security awareness and automation capability of a civil society. The best defensive strategy is to embed security awareness at all level of daily information exchange practice. This is the area that OCA-compliant process excel at doing, raising awareness of the latest system-level technologies. Knowledge is power, the ability to continuously introduce information and cybersecurity literacy through a common process model pioneered by CICD/DevSecOps can be particularly beneficial to early adopters. Whichever organization, even individuals that started practicing and adopting these advanced toolchains for personal or organizational productivity would gain tremendous competitiveness over others who don’t.

### Tools:

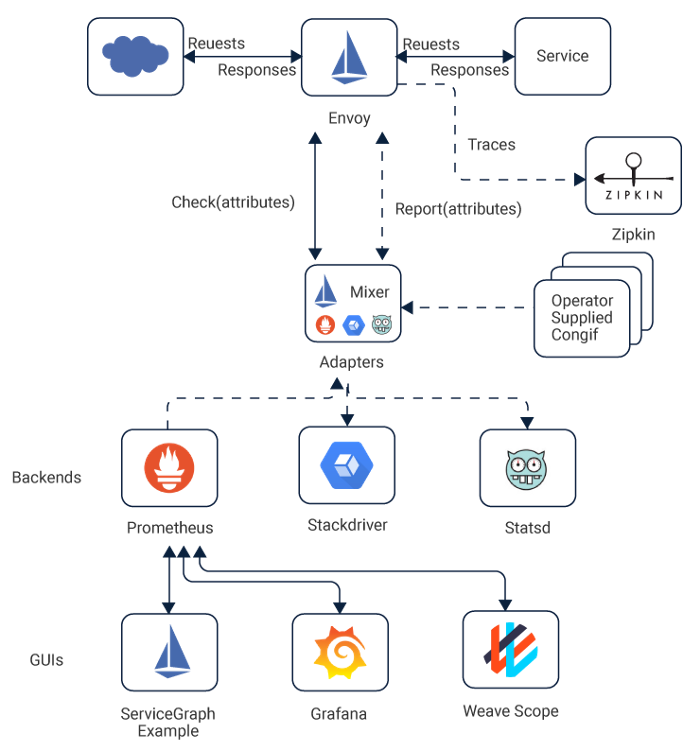
#### Cyberspace decomposed into Data Plane and Control Plane

Data centers, network operators Internet Service Providers

[Data Plane and Control Plane](https://miro.medium.com/max/700/0*TqtI0ugMrqZpopd5.png)



#### Monitoring



#### Open Sourced Coordination Tools

#### Password Management and Authentication Services

#### Encryption Technologies

#### Automated Security Model Verification

#### Machine Learning and Operational Data Sources

## Expected Challenges

The key feature of Omnia Cybersecurity Architecture (OCA) is that it obeys the Principle of Information Symmetry at all levels. 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.

# 

# Glossary

##### Principle of Information Symmetry:

An OCA-defined system design principle, emphasizing the preference to share and rapid synchronize technical information and operational metadata across trusted parties. The information shared doesn’t include commercialized intellectual properties and personal or protected information.

# 

# References

Richard Stallman, Free Software, Free Society, [electronic media](https://www.gnu.org/philosophy/fsfs/rms-essays.pdf) in PDF form, last accessed: July 10, 2020

Philip Windley, Digital Identity, Oreily Media, 2008

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

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

Veritis, [Transitioning from DevOps to DevSecOps: integrating “Security as Code” culture to DevOps](https://www.veritis.com/solutions/devops/devsecops-services/), last accessed July 10, 2020

Gartner, [Integrating Security into the DevSecOps Toolchain](https://www.techwire.net/sponsored/integrating-security-into-the-devsecops-toolchain.html), published 2019, last accessed July 10, 2020

XebiaLabs, [DevSecOps: The Missing Link in Delivering on the Promise of Business Velocity](https://www.slideshare.net/xebialabs/devsecops-the-missing-link-in-delivering-on-the-promise-of-business-velocity?from_action=save), published 2018, last accessed July 10, 2020

Cuelogic Technologies, [Istio Service Mesh: The Step by Step Guide](https://itnext.io/istio-service-mesh-the-step-by-step-guide-adf6da18bb9a), published 2019, last accessed July 11, 2020

Phil Windley 2018, [Multi-Source and Self-Sovereign Identity](https://www.windley.com/archives/2018/09/multi-source_and_self-sovereign_identity.shtml), published 2018, last accessed July 11, 2020

1. According to Wikipedia, the political consulting firm, [Cambridge Analytica](https://en.wikipedia.org/wiki/Cambridge_Analytica) Ltd, combined data analysis with proactive communication techniques to influence electoral processes in multiple nations. [↑](#footnote-ref-0)
2. CICD stands for Continuous Integration and Continuous Delivery/Deployment. [↑](#footnote-ref-1)
3. DevSecOps is an extension of DevOps, which means Development + Security + Operations. [↑](#footnote-ref-2)
4. It is important to note that activities in private cyberspaces should not be publicized. [↑](#footnote-ref-3)
5. Richard Stallman, Free Software, Free Society, [electronic media](https://www.gnu.org/philosophy/fsfs/rms-essays.pdf) in PDF form, last accessed: July 10, 2020 [↑](#footnote-ref-4)
6. 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 [↑](#footnote-ref-5)