# How Software Defined Networking (SDN) Supports Mental Models for Cyber Security Defenders

WJ Hutton III, MD Hadley

*Pacific Northwest National Laboratory*
*Richland, WA U.S.A.*

*E-mail:* *william.hutton@pnnl.gov*, *mark.hadley@pnnl*

***Abstract****: Software Defined Networking for Operational Technologies, abbreviated as OT-SDN in this paper, is a leading technology to secure critical infrastructure and command and control (C2) networks. As the name implies, OT-SDN networks are programmable, which allows system owners to utilize the characteristics of their physical processes to inform the security of their network. In this paper we will provide an overview of several mental models for cyber security defenders. Then explore how OT-SDN supports the thought process and workflow of cyber defenders. We will also examine the corollary, how OT-SDN disrupts the actions of cyber attackers.*

**Keywords:** *Software Defined Networking, Operational Technology, Network Security, Cyber Security, OODA Loop*

## 1.0 Introduction

Security is an age-old problem. However, the subfield of cyber security is relatively new because computers are a modern invention, but we can apply strategy and tactics learned long ago. For example, the "Five D's" from physical security: deter, detect, deny, delay, and defend also apply to cyber security. Over the past decade or two, cyber security has largely focused on detect—finding cyber solutions that detect threats. Setting aside the problem of accuracy (e.g., false positive alarms, missing true positives, etc.) the emphasis on detection has two serious flaws.

The first flawed assumption is that if we could just get more sources of data, we could detect the right indicators that would allow us to respond to a threat. This belief has led to a deluge of information and overwhelmed cyber defenders. Second, one should not assume that detection leads to action. Over the years, response times have improved, but they are still measured in months. Often the first indication of a cyber-attack is the impact (e.g., a significant compromise or exploitation), which is the conclusion of the attack, leaving no time for defence, only recovery. When we frame these shortcomings in the perspective of the OODA loop model, you can see that the first assumption means the "orient" and "decide" phases are missing, and the second assumption means that the "act" phase is ineffective or absent.

The deny-by-default approach of SDN-based network greatly reduces the amount of observations time required in an OT network. The only network communications allowed in an OT-SDN network conform to a specification defined by the SDN flow rules, which means that observation occurs at network line-rates within the SDN switches. The absence of unexpected or undefined network conversations within OT networks makes the observation and orientation phases of the OODA loop trivial and automates the decision and act phases of the OODA loop at network speed.

This paper is broken into three sections. Section 2.0 introduces several mental models from the physical security domain that are applicable to cyber security. Section 3.0 is an introduction to OT-SDN. Aside from a brief introduction to SDN, this section describes how operational technology (e.g., industrial control systems, SCADA, IoT and cyber-physical systems) differ from traditional IT networks. Section 4.0 melds the ideas of mental models and OT-SDN, showing how software defined networking both supports defenders and interrupts attackers' mental models.

## 2.0 Mental Models for Security

In order to think critically about something complex, we often use a model to abstract needless details and focus on what is of critical importance. When doing so, one must remember the famous quote of statistician George Box, "All models are wrong. Some models are useful." [1]. In the sections below, we introduce several useful models. First, the **OODA loop**, which models decisions and actions in adversarial competitions such as aerial combat. Next we introduce **decision sticks**, which are an offshoot of the OODA loop and focus on comparative times to execute one cycle of the OODA loop for each combatant. The **Cyber Kill Chain®** developed by *Lockheed Martin* generalizes the steps needed to compromise an IT system. Finally, we introduce the **Timely Detection** model, developed by the United States Department of Energy to safeguard special nuclear material. By adopting all four models, cyber defenders have a mental framework to design, implement, and maintain cyber security policy and security controls as well as incident response and recovery. After a brief introduction to software defined networking, the second half of this paper connects SDN functionality to these models to show how SDN can be implemented to automate some cyber defence functions and reduce the cyber defender's cognitive load

## 2.1 The OODA loop

One such useful model is John Boyd's "OODA loop" (see Fig. 1). Col. John Boyd was a fighter pilot in the Korean War and taught his OODA loop as a model for thinking during aerial combat to many pilots at the USAF Weapon School. Boyd's OODA loop was so effective it has been widely applied to many diverse fields outside of the military where adversarial thinking is common, including; sports psychology, finance, and litigation. The OODA loop has applications wherever tactical or strategic thinking is required, including cyber security.

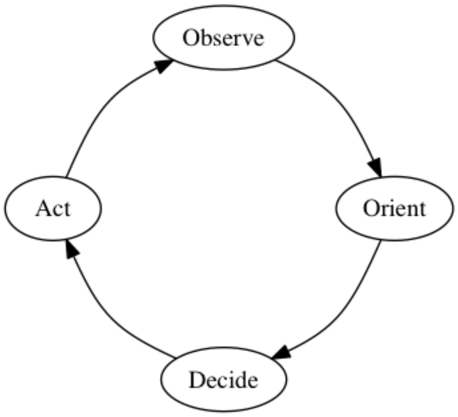

*Figure 1. The OODA loop*

The four steps of the OODA loop are **observe**, **orient**, **decide**, and **act**. The four steps are repeated until one side wins. We all practice the OODA loop thousands of times a day, usually unconsciously. Simply walking through a crowded space (e.g., a shopping mall or airport) is a good example of executing the OODA loop, whether you know you are doing it or not. We observe many people, but only a few of those people are an immediate "problem" that requires a decision and an action. We orient ourselves by focusing on these problems—people we may collide with if neither of us takes any action. We decide to alter our course (e.g. speed up, slow down, shift left, stop, etc.). Then we execute the decided upon action. We repeat the OODA loop by observing the outcome of our action and repeat the process until we have accomplished our goal of moving through the crowd without bumping into anyone. By the time we reach adulthood, most of us are so good at this that it becomes almost unconscious. But for tasks we have less mastery over, managing airspeed and altitude in a two-circle fight to place our aircraft on a bandit's six, mental models like the OODA loop are essential to success.

Of course, the OODA loop is more useful when we purposefully execute it. The OODA loop scales well in both scale of conflict and force escalation. It is equally useful for brief, violent encounters between two unarmed individuals to strategic conflicts between nation states using nuclear weapons (e.g., the Cuban Missile Crisis in 1962).

## 2.2 Decision sticks

Decision sticks are a martial arts application of the OODA loop. The karateka that cycles through their OODA loop the fastest has the best chance to win[5]. A decision stick measures time vertically, while indicating when orientation, decision, and action occur. In Figure 2.a., the base of a decision stick indicates the start of the observation phase of an OODA loop. The time it takes to transition from general observation to specific orientation is shown as a tick mark on the left side of the forming rectangle in Figure 2.b. The time taken to make a decision from the available choices is indicated by a tick on the right side of the forming rectangle in Figure 2.c. When the decided upon action is finally executed, the top of the rectangle completes the decision stick, as in Figure 2.d. Attackers usually have shorter decision sticks compared to defenders, because the defender must execute their OODA loop in response to the action of the attacker.

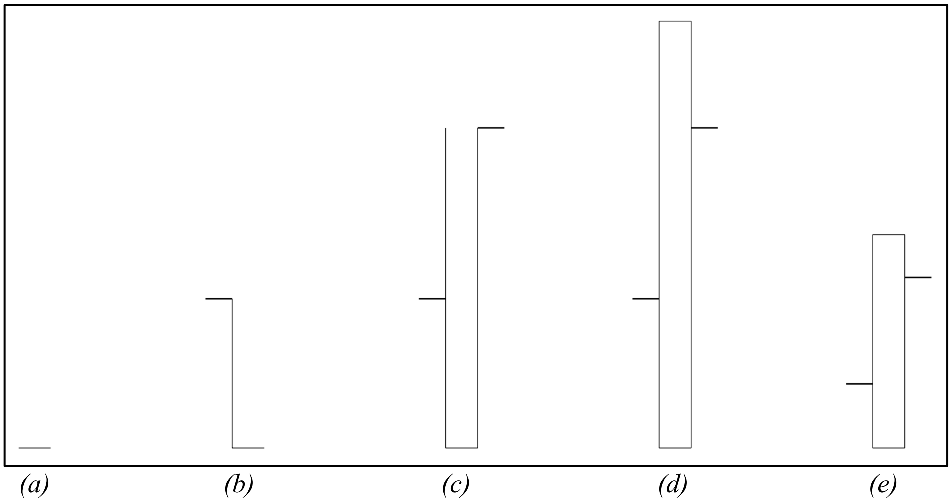

*Figure 2. Construction of a decision stick*

Strategies to reduce cycle time include faster orientation, faster decisions, and more effective actions. Figure 2.e shows a shorter decision stick with faster orientation, decision, and action compared to Figure 2.d.

In an adversarial contest, the shortest decision stick usually wins. If you fail to observe something, your decision stick is "stuck" at the bottom, leaving little to no time to orient yourself to what is important. Likewise, taking too long to make a decision may drive the right side of your decision stick past the point where you can take an action. By altering the height of the decision stick, or changing where the left or right sides of the stick appear, we can illustrate many different flaws in strategic thinking, such as orienting on the wrong thing, taking too long to make a decision, or being forced to take a suboptimal action due to not enough decision time.

## 2.3 The Cyber Kill Chain

The U.S. defence contractor, *Lockheed Martin*, developed the Cyber Kill Chain [6] to model the necessary steps an advanced persistent threat typically takes to accomplish an objective, such as loss of confidentiality, loss of integrity, or loss of availability. The Cyber Kill Chain is:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives

Reconnaissance can occur on or off network and includes technical methods to map network topologies such as ping sweeps, port scans, and vulnerability scans as well as harvesting information from social networking sites like LinkedIn. Weaponization couples an exploit to a vulnerability in a deliverable payload. The aptly named delivery phase delivers the malicious payload via traditional networking methods, or via "sneaker net" on a USB device. Exploitation executes the delivered malware payload to take advantage of one or more discovered vulnerabilities to establish initial access. All the steps in the Cyber Kill Chain up to this point are typically labour intensive and prone to detection. Therefore, the advanced persistent threat seeks easier access, and that is what the remaining three steps focus on. The installation of malware to establish persistent command and control access that enables actions on the objective. Once the final three steps are accomplished, the adversary "pwns" (i.e. owns) the asset.

The Cyber Kill Chain allows a cyber defender to determine where an adversary is in their attack process and what their next steps will likely be. Pairing this mental model with a model for adversarial action such as the OODA loop, decision sticks, or timely detection will enable the defender to take action to respond to the attack.

## 2.4 Timely detection

The Timely Detection model is a method of quantitatively evaluating a physical security system developed by the U.S. Department of Energy. Pacific Northwest National Laboratory has done extensive research to extend the Timely Detection model include cyber systems and the interactions between physical systems and cyber systems [3]. A **system effectiveness** score, which is calculated as a percentage, considers three primary numbers; probability of detection, amount of delay provided, and response time.

First, a graph for each layer of the system is created. For the physical layer, a node in the graph represents a physical location. Edges in the graph connect physical locations. Each edge is decorated with performance metrics for any security controls that may be encountered while transitioning from one location to another. Given a security control, the primary metrics are probability of detection and amount of delay provided. These metrics may vary depending on the threat encountering them and the threat's tools, tactics, and procedures, as well as the adversary's operating mode. An adversary attempting to avoid detection will move much more slowly and deliberately. Once an adversary is detected, they will shift from stealth to speed.

Using Figure 3 as a simple example, we see the physical model of a house. The goal of an adversary outside the house is to steal a cookie from the kitchen. For simplicity, we only list one set of metrics for a skilled, stealthy adversary. For the same adversary operating with speed instead of stealth, a red set of metrics would decorate the edges, with generally lower delay, but higher probabilities of detection. For an unskilled adversary, the locks on the front and back door may provide far more delay than two minutes (i.e. 120 seconds) if the lock is to be picked. The probability of detection may be much higher if the door must be forced open instead of picking the lock.

Beginning from the "Outside" node and moving to the "Kitchen", there are multiple walks of the graph, each with an associated probability of detection and total amount of delay. Entering from the kitchen window would take 40 seconds with a 30% chance of detection. Picking the lock on the front door then moving through the living room to the kitchen has the same probability of detection and takes two minutes and ten seconds. While undetected, delay for the adversary is merely a nuisance. They do not care if it takes them longer to accomplish their goal if they can remain undetected. Therefore, the best approach for the adversary is to pick the lock on the back

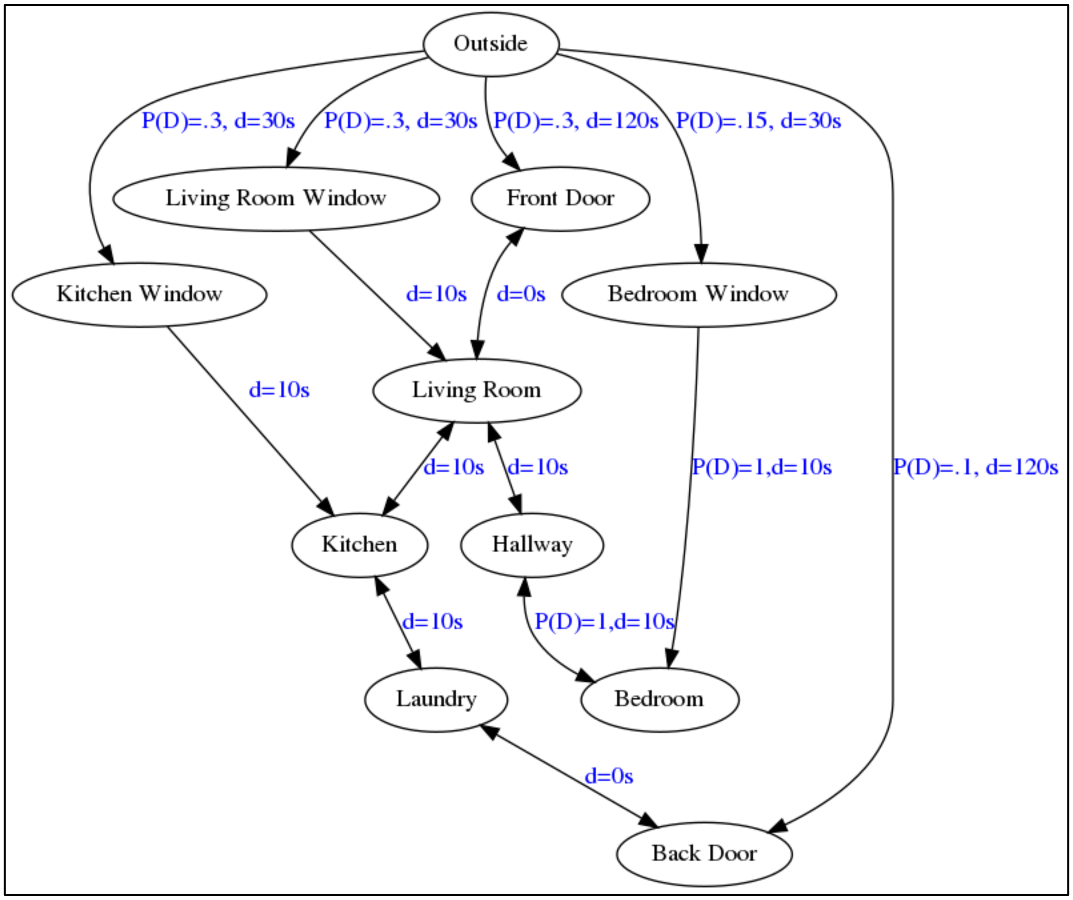

*Figure 3. Timely Detection model, physical*

door, which only has a 10% chance of detection, then move through the laundry room to the kitchen to steal the cookie.

Assuming the homeowner is in the bedroom, there is a 100% chance of detection if the adversary enters through the bedroom window or moves from the hallway into the bedroom. The other important metric is the response time. It takes 30 seconds to move from the bedroom to the kitchen, but only 10 seconds for the adversary to move from the open kitchen window into the kitchen. Additional delay must be added to compensate for the homeowner's 30 second response time.

This model can be extended to cyber systems. The graph could show physical or logical network connections. Implemented security controls from U.S. NIST SP 800-53[4] "Security & Privacy Controls for Federal Information Systems and Organizations" are evaluated for probability of detection and amount of delay they provide for various threats. NIST's SP 800-82 [9] "Guide to Industrial Control Systems (ICS) Security" has helpful information for applying the IT guidance in 800-53 to OT systems.

Multiple responses may be possible. Only the slowest response should be evaluated. If the system effectiveness is satisfactory for a slow response, it will remain unchanged by a faster response. Finally, response effectiveness is considered to be 100% effective against a specified threat. The specific threat a response is designed to repel with absolute certainty is explained in a Design Basis Threat (DBT) document. Obviously, the information in the DBT is sensitive.

## 3.0 Introduction to Operational Technology—Software Defined Networking (OT—SDN)[1]

SDN is both a new network architecture and a new network paradigm that simplifies network management by abstracting the control plane from the data forwarding plane. Figure 5 illustrates the building blocks of SDN, which are discussed in the following four subsections.

### 3.1 Control plane

At the core of SDN is a controller that embodies the control plane. Specifically, controller software determines how packets (or frames) should flow (or be forwarded) in the network. The controller communicates this information to the physical network devices, which constitute the data plane, by setting their forwarding tables. Each forwarding table contains a list of the authorized network flows permitted within the SDN. This enables centralized configuration and management of a network. Many open source controllers such as Floodlight (http://www.projectfloodlight.org/ floodlight/), NOX (http://www.noxrepo.org), and Ryu (http://osrg.github.io/ryu/), are readily available.

### 3.2 Data plane

The data plane consists of network devices that replace switches and routers. In SDN, these devices are very simple Ethernet packet forwarding devices with a communications interface to the SDN controller that is used to receive forwarding information. Many vendors today provide packet forwarding devices that are SDN-enabled. The data plane can efficiently process network traffic at line speeds because the data plane devices do not have to compute network routing decisions—they only have to execute the rules previously provide by the SDN controller.

[1] Section 3.0 authored by M. Hadley originally appeared as “Software-Defined Networking Address Control System Requirements” in “Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2018”. April 2014.

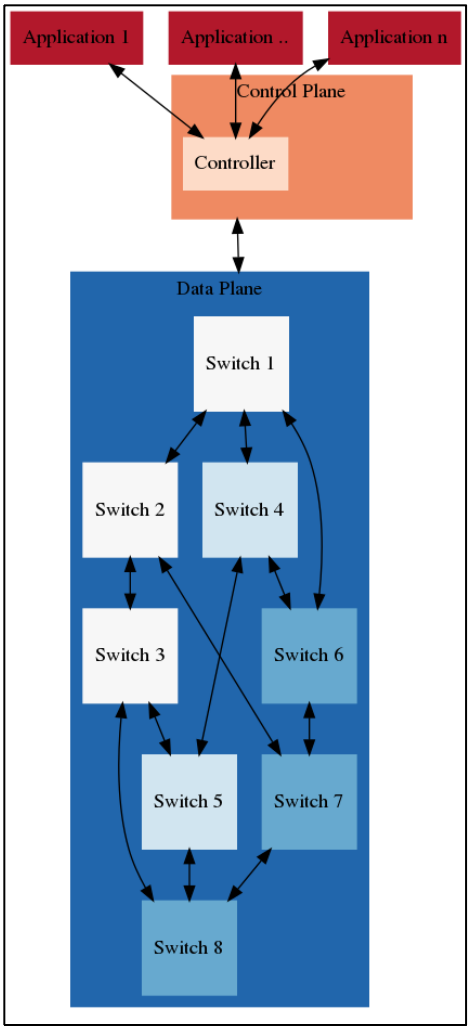

Figure 5. Software defined networking

## 3.3 Communications interface

SDN requires a communications interface between network devices and the controller, as is evident from the description of control and data planes. A standardized interface between them allows bidirectional operation between a controller and different types of network devices. The OpenFlow switch protocol [7] is one such standardized interface that is managed by the ONF [8] (Open Networking Foundation) and has been adopted by major switch and router vendors. However, it should be noted that OpenFlow is just a building block in the SDN architecture and there are other open IETF (Internet Engineering Task Force) standards or vendor-specific standards that are either already available or are being developed.

## 3.4 SDN services

In SDN architecture, the controller can expose an API (Application Programming Interface) that services can use to configure the network. In this scenario, the controller can act as an interface to the switching fabric while the control logic resides in the services using the controller.

Depending on the SDN controller being used, the interfaces may be different. Controllers and their APIs can be tailored to meet the needs of an application domain. A controller that is designed and optimized for data centres, for example, may not be suitable for control networks in the electric sector and vice versa. The application domain specific to the industry it is used in will determine the overall system requirements. Trade-offs between optimizations like single instruction speed or parallel processing determine the best interfaces to use for a given application.

While SDN is commonly used for monitoring and programmatically changing network configurations, the centralized nature of SDN is also well suited to meet the security, performance, and operational requirements of control system networks. OT networks are designed to do specific jobs for many years with as little change as possible.
With the help of SDN, operators can take advantage of this knowledge to preconfigure network paths and effectively create virtual circuits on a packet switching network. Utilities can design the virtual circuits they require for communication between devices and lock down communications paths. This type of approach enhances security by reducing the attack surface and provides a clear approved baseline that can be continuously monitored to ensure it remains unchanged.

## 3.5 A New Paradigm

SDN is a new approach to the configuration, operation, and management of network systems. This architectural change is revolutionizing the management of large-scale enterprise networks, cloud infrastructures, and data centre networks to better support the dynamic changes required many times a day. The reasons SDN has been adopted so much in the corporate IT world are also why we believe it can have a significant impact in the management of OT networks. SDN allows a programmatic change control platform, which allows the entire network to be managed as a single asset, simplifies the understanding of the network, and enables continuous monitoring in more detail. Compared to IT networks, OT networks are much more static, while the corporate world is more dynamic. That is, OT network flows are more consistent and continuous than the ever-changing nature of an IT network flow snapshot. This is largely due to the physical layer of the OT system being purpose-built and consisting primarily of machine-to-machine communications, while corporate communications are mostly human to machine or human to human. SDN architecture is applied differently in OT. However, SDN architecture is able to optimize for both use cases. The fundamental shift in networking brought by SDN is the decoupling of the systems that decide where the traffic is sent (i.e. the control plane) from the systems that perform the forwarding of the traffic in the network (i.e. the data plane).

The traditional network deployment process begins with designing the topology, configuring the various network devices, and, finally, setting up the required network services. In order to achieve the optimal usage of network resources, the application data must flow in the direction of the routes determined by the routing and switching protocols. In large networks, trying to match the network discovered path with an application desired data path may involve changing configurations in hundreds of devices with a variety of features and configuration parameters. In addition to this, network administrators often need to reconfigure the network to avoid loops, gain route convergence speed, and prioritize a certain class of applications.

This complexity in management arises from the fact that each network device (e.g., a switch or router) has control logic and data forwarding logic integrated together. For example, in a network router, routing protocols such as RIP (Routing Information Protocol) or OSPF (Open Shortest Path First) constitute the control logic that determines how a packet should be forwarded. The paths determined by the routing protocol are encoded in routing tables, which are then used to forward packets. Similarly, in a Layer 2 device such as a network bridge (or network switch), configuration parameters and/or STA (Spanning Tree Algorithm) constitute the control logic that determines the path of the packets. Thus, the control plane in a traditional network is distributed in the switching fabric (i.e. network devices), and as a consequence, changing the forwarding behaviour of a network involves changing configurations of many (if not all) network devices.

## 4.0 How OT-SDN Supports Mental Models for the Cyber Defender

We will use the Cyber Kill Chain described in Section 2.3 above to frame the attacker actions. At each step of the Cyber Kill Chain, we will use the OODA loop described in Section 2.1 above to discuss the defender options.  In each instance we will describe how OT-SDN supports the cyber defender.  Then in Section 5.0 below we reverse the analysis to illustrate how OT-SDN disrupts the attacker.

### 4.1 Recon

In this hypothetical example, assume a cyber activist is targeting a nuclear generation facility. The attacker’s initial goal is to remotely trigger an automatic shutdown (i.e. a SCRAM) at the generation facility.  This is highly unlikely due to strict regulatory requirements for disconnected (i.e. air gapped) systems, but the attacker may not now that.  A secondary goal will be to shift from OT to IT to create a public perception problem for the utility by hacking their web site.

The first recon actions likely occur off network (e.g., LinkedIn, IANA WHOIS search, etc.) or through normal usage (e.g., accessing the utility’s public facing website) to gather the first pieces of information; physical addresses, public IP addresses, and names of board members, administrative and technical contacts, phone numbers, email addresses, etc.  All of this information is useful for phishing or social engineering attacks.

Because these activities primarily happen off network, the cyber defender cannot observe these activities and their OODA loop does not yet begin.

A distant adversary may ping sweep the Class C subnet associated with the utility’s public website at this point.  A properly configured SDN controller would explicitly prohibit any public IP address from communicating with any IP address on the network that was not offering public services like HTTP or HTTPS.  In this case, the malicious network traffic never makes it onto the network.  Likewise, if the adversary performed a port scan on the public web server, none of the network packets addressed to any socket other than port 80 and or port 443 would ever even make it onto the network.

In this case, there is nothing for the cyber defender to observe or orient towards. SDN can be configured to forward network packets that do not match SDN flow rules for situational awareness and intrusion detection purposes, but these activities take on new context with SDN.

You may want to refer to Section 5.1 to see how SDN disrupts recon for the attacker before continuing.

### 4.2 Weaponization

With the recon phase severely limited, there are few options for weaponization. The adversary is forced to look for vulnerabilities in the exposed network devices, services, and protocols. If the web server application is current on security updates and patches, there may not be any known vulnerabilities. If the attacker is not capable of finding their own zero day, the attack is neutralized. If the attacker does have the resources to find and weaponize a new vulnerability, SDN has increased the cost of the attack in terms of both time and money. This is an asymmetric advantage for the defender.

Because weaponization and testing both occur off network, the defender has no OODA loop to exercise at this point and must wait for the delivery of the payload to begin their OODA loop. However, OT-SDN's deny-by-default paradigm reduces cognitive load for the defender and allows the defender to orient solely on activity defined by SDN controller flow rules.

### 4.3 Delivery

Because of the effectiveness of OT-SDN, even with the IT portion of our scenario, some accommodations must be made. Assume an older version of the Apache httpd software is running on the web server. Also assume that this older version of Apache has a known remote buffer overflow vulnerability which the attacker has weaponized in the previous step of the Cyber Kill Chain.

It is common for payload deliveries to have an anomalous size. Consider CVE-2002-0082, which is obviously an older vulnerability, but the nature of buffer overflows is consistent. More data must be sent than a variable can hold. The payload itself typically includes a reverse shell or some other method to initiate a connection from the target back to the attacker. The size of the reverse shell [10] used with the CVE-2017-0144 (i.e. Eternal Blue) is 751 Bytes. Most HTTP Requests are much smaller than the HTTP Response they initiate. More data may be expected for the HTTP POST method. Similar norms exist for protocols both in general terms as well as specific patterns for an individual organization. These patterns in OT are not just predictable but often calculatable. After identification, these patterns tend to be static and unchanging over time. OT-SDN can be programmed to ensure observed traffic adheres to these patterns. This severely restricts malware delivery options because there is no overhead for malicious code to be transmitted between network devices in an OT-SDN network.

In terms of the OODA loop, OT-SDN automates all four steps. OT-SDN observes the network traffic, orients on the source, destination, protocol, timing, and size of the packet using flow rules, and acts by dropping network packets that do not conform to the definition of normal.

### 4.4 Exploitation

Because OT-SDN strictly enforces expected network communication between devices with flow rules, traditional attack methods are stopped early in the Cyber Kill Chain. There are far less opportunities for attackers to exploit the system. Attacker exploitation efforts are restricted to normal operating behaviour. This means packet fuzzing and covert channels. OT-SDN allows cyber defenders to shape to topology of the digital battlefield, forcing attackers to exploit known points in the network. OT-SDN frees the defender to focus observation and orientation on these key points. Because there is less load on the observe and orient steps of the OODA loop, the defender has fewer decisions to make and can define procedures for pre-planned actions. These advantages shorten the defender's decision stick.

### 4.5 Installation

Recall the first four steps of the Cyber Kill Chain are about establishing initial access. The last three steps are all about what an attacker does after they gain initial access. OT-SDN disrupts initial access and prevents persistent access. It becomes harder and harder to describe how OT-SDN supports mental models for cyber defenders. When the attack is disrupted early in the Cyber Kill Chain, the subsequent steps become irrelevant.

The key concept is that OT-SDN simplifies observation and orientation by eliminating malicious network traffic and automates decisions and actions, freeing up cyber defenders to focus on detection of new attack techniques, which will come at a slower pace.

### 4.6 Command & Control

Command and control involves signalling from the attacker's computer to the target to accomplish their actions on the objective. With no persistent access, there are no command and control signals to observe. The OT network becomes hyper quiet. Any misconfiguration or other maintenance issues spike from the low noise floor. The defender can rapidly orient towards these issues and make rapid decisions and take quick action.

### 4.7 Actions on Objective

By interrupted the Cyber Kill Chain before persistent access can be established, we don't expect remote actions on objectives within an OT network. We have piloted our OT-SDN approach at four locations throughout the United States. To date we have observed no indicators of compromise and strict flow rules have allowed defenders to observe and orient to several previously unknown misconfigurations that led to service interruptions.

## 5.0 How OT-SDN disrupts Mental Models for the Cyber Attacker

This section describes how OT-SDN disrupts the attacker's mental model and interrupts the Cyber Kill Chain. You may find it helpful to read the corresponding section in Section 4.0 above then return to each subsection below.

### 5.1 Recon

SDN restricts the information that an adversary can discover on network through ping sweeps and port scans. This limits the attackers observe step of the OODA loop and restricts the options to orient towards. Decision times are lengthened due to the limited information and available actions are restricted. Given that all networks are different, it is hard to quantify the impact, but assuming a half full Class C subnet (i.e. 126 hosts) with just five services running on each host, that is 630 points to interact with the attack surface. The scenario in Section 4.1 reduces that number to just two (assuming the web server serves both HTTP and HTTPS content)—a 99.997% reduction in attack surface.

### 5.2 Weaponization

With restricted information, the attacker has fewer available decisions and fewer possible actions. The defender's OODA loop will lengthen as they attempt to observe additional information, look for new orientations and extend their decision making. The OODA cycle may actually break without anything to orient towards or without any meaningful decisions or actions to take.

The majority of attacker actions will be ineffective due to SDN's deny-by-default paradigm. In most cases, the only thing the attacker can do is behave like a normal, authorized network device, which by definition is not abnormal or malicious. This greatly extends the attacker's decision sticks. Remember, the shortest decision stick usually wins [5]!

### 5.3 Delivery

When it comes to delivery of malicious payloads, the attacker will observe their actions have no effect. OT-SDN flow rules already limit network traffic by address. If somehow the attacker was able to spoof the identity of an allowed host, the traffic they send from that host may only reach other predefined hosts. Furthermore, the traffic must conform to expectations of normal; the correct protocol, the correct frequency, and the correct size. Any deviation from these expectations will result in the packet being dropped.

Finding delivery of a malicious payload impossible, the attacker will have to return to the limited information gathered in the recon phase and look for another vulnerability to weaponize.

### 5.4 Exploitation

With no options for malicious code delivery, the attacker must repeat the earlier stages of the Cyber Kill Chain. The automated actions of OT-SDN force the attacker to try and find malicious use of normal functions. This greatly slows the attack speed of the attacker and increases the probability of detection as the attacker iterates the lower steps of the Cyber Kill Chain, wasting resources on incomplete recon and ineffective weaponization.

### 5.5 Installation

Similar to the previous step of exploitation, installation efforts will largely be failed actions for the defender. The effect is repeated effort at lower steps of the Cyber Kill Chain. Recall that the attacker has not actually achieved their goal until step 7. Any interruption before step 7 is a defeat for the attacker. This leads to longer observation, orientation, and decision steps in the attacker's OODA loop which means longer decision sticks—with no effective action to complete the loop.

### 5.6 Command & Control

Command and control is interrupted by no persistent access for the attacker. This will drive attackers to single-use windows of initial vulnerabilities that used to offer initial access.

### 5.7 Actions on Objective

With no effective actions, reduced decisions, and limited observation, attacker's traditional workflow identified by the Cyber Kill Chair are disrupted. Actions on objectives such as loss of confidentiality, loss of integrity, and loss of availability must be reinvented with far less options for the attacker.

## 5.0 Conclusion

Securing networks within critical infrastructure is a unique cyber security challenge. These networks are usually a combination of analogue and digital components and may span multiple decades of differing technologies. Initial design goals were often functional, with little to no consideration for security. Maintaining critical infrastructure capabilities can preclude large scale technology replacements, reconfigurations, or even patching. Each of these restrictions is a contributing factor to increased vulnerability and increased adversarial impact. Over 90% of all cyber security attacks begin with phishing and include some type of lateral movement [2]. SDN has been proven to be an effective mitigation by taking a deny-by-default approach in deterministic network environments.

SDN greatly reduces the workload for cyber defenders by trivializing half of the steps in the OODA loop and automating the other two phases. Because the shortest decision stick tends to win in adversarial confrontations, SDN also allows the defender to interrupt the adversary's OODA loop by making decisions and taking actions faster than a human can observe and orient to them.

## 6.0 Acknowledgements

The work described in this paper was conducted under the sponsorship of the U.S. Department of Energy by cyber security researchers and engineers at Pacific Northwest National Laboratory. The authors extend their gratitude to the Cybersecurity for Energy Delivery Systems (CEDS) Division within the Cybersecurity, Energy Security, and Emergency Response (CESER) Office and to the U.S. Department of Defense stakeholders, electric utilities, vendors and engineering firms who have partnered with us on our SDN projects.

## 7.0 References

[1] Box, G. E. P. (1976), *"Science and statistics"* *(PDF)*, *Journal of the American Statistical Association*, **71**: 791–799, *doi*:*10.1080/01621459.1976.10480949*

[2] Frinke, D., “Keynote Address Northwest Cybersecurity Symposium”. Pacific Northwest National Laboratory, Discovery Hall. April 8 – 10, 2019.

[3] Hutton, William J. “Computer-Implemented Security Evaluation Methods, Security Evaluation Systems, and Articles of Manufacture”. 28 July 2015.

[4] Joint Task Force Transformation Initiative. “Security and Privacy Controls for Federal Information Systems and Organizations”. NIST. April 2013. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[5] Kane, L., and Wilder, K., “The Way to Black Belt” (pgs. 114-115). YMAA Publication Center, Inc. 2007.

[6] Lockheed Martin, “The Cyber Kill Chain”, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[7] Open Network Foundation, “OpenFlow Switch Specification” version 1.5.1. March 2015. https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf

[8] Open Network Foundation. Accessed June 29, 2020. https://www.opennetworking.org/

[9] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., and Hahn, A. “Guide to Industrial Control Systems (ICS) Security. NIST. May 2015. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[10] Worawit Wang, “MS17-010” (Eternal Blue vulnerability testing tools). Accessed June 29, 2020. https://github.com/worawit/MS17-010