Distribution Statement A: Approved for public release; distribution is unlimited.

VOLUME 8 | NUMBER 1 | 2024

CSIAC JOURNAL

A DEFENSE-IN-DEPTH AND LAYERED APPROACH TO

SOFTWARE SUPPLY CHAIN SECURITY

PAGE 19

CSIAC JOURNAL

Volume 8 // Number 1 // 2024

Editor-in-Chief:
Gregory Nichols

Sr. Technical Editor:
Maria Brady

Graphic Designers:
Melissa Gestido, Katie Ogorzalek

The CSIAC Journal is a publication of the Cybersecurity & Information Systems Information Analysis Center (CSIAC). CSIAC is a DoD Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) with policy oversight provided by the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E). CSIAC is operated by the SURVICE Engineering Company.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or CSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or CSIAC and shall not be used for advertising or product endorsement purposes.

ISSN 2836-7383 (Print) // ISSN 2836-7391 (Online)

Distribution Statement A:
Approved for public release; distribution is unlimited.

On the Cover:
Digital Art Rendering *(Source: 123rf.com).*

CSIAC Cybersecurity & Information Systems Information Analysis Center

ABOUT CSIAC

Who We Are

A DoD Information Analysis Center comprised of scientists, engineers, researchers, analysts, and information specialists.

What We Do

Generate, collect, research, analyze, synthesize, and disseminate scientific and technical information (STI) to DoD and federal government users and industry contractors.

Why Our Services

To eliminate redundancy, foster collaboration, and stimulate innovation.

CSIAC SERVICES

Subject Matter Expert (SME) Connections

Access to a network of experts with expertise across our technical focus areas.

Technical Inquiries (TIs)

Up to 4 hours of FREE research using vast DoD information resources and our extensive network of SMEs.

Specialized Task Orders

Research and analysis services to solve our customer's toughest scientific and technical problems.

Webinars & Events

Our webinars feature a technical presentation from a SME in one of our focus areas. We also offer key technical conferences and forums for the science and technology community.

STI Collection

Our knowledge management team collects and uploads all pertinent STI into DTIC's Research & Engineering Gateway.

Information Research Products

The Cybersecurity & Information Systems Digest, state-of-the-art reports, journals, TI response reports, and more available on our website.

CONTACT CSIAC

IAC Program Management Office

8725 John J. Kingman Road
Fort Belvoir, VA 22060
Office: 571.448.9753

CSIAC Headquarters

4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600
Fax: 410.272.6763
Email: contact@csiac.org

CSIAC Technical Project Lead

Phil Payne
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600

IN THIS ISSUE

IMPROVING THE U.S. AIR FORCE'S

CYBER DEFENSE STRATEGY

BY ANTHONY FRANKS

(PHOTO SOURCE: DIGITAL ART RENDERING FROM 123RF.COM AND U.S. AIR FORCE)

INTRODUCTION

April 2007 marks the month when the internet became weaponized [1]. In Estonia's capital city of Tallinn, the government decided to move a bronze statue of a Russian soldier from the city center to a war memorial cemetery on the outskirts of town (Figure 1). They wanted to move the statue during the 60th anniversary of its erection in 1947, which memorialized the sacrifices of Russian soldiers liberating eastern Europe from the Nazis.

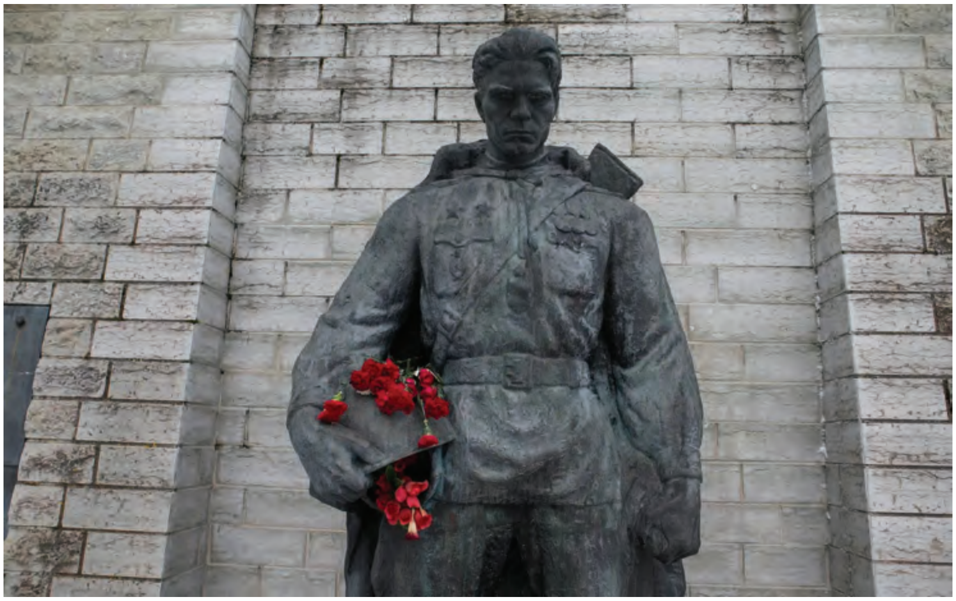


Figure 1. Russian Soldier Statue *(Source: Postimees/Scanpix)*.

Amidst protests, a targeted distributed denial of services (DDoS) attack struck banking, government websites, and small businesses, taking these government and commercial services offline for several weeks. The Estonian government brought services back online, but this event marked the first time the world had seen a "cyberattack." Leading experts attributed this DDoS attack to Russian organizations. Fourteen years earlier, another momentous cyber event took place but was not limited to just Estonian citizens—this event changed the world forever.

The World Wide Web (WWW) became first available for public use and consumption in April 1993 [2]. It was the brainchild of researcher Tim Berners-Lee while working at CERN, a Swiss physics lab. But the original internet, predating the WWW by 24 years, was a military invention called the ARPANET [3]. Built in 1969, the ARPANET demonstrated data being transferred via computers outside a local network for the first time. Its name came from an agency called ARPA, predecessor of the Defense Advanced Research Projects Agency (DARPA). Even though the United States has had an internet since 1969, when the WWW opened its aperture to the world, the public and private sectors became so interconnected that it is now considered by some countries as a human right.

From its earliest days, organizations utilizing the ARPANET's data transfer capability knew each other when they communicated on the network, and trust was implied. But since the opening of the WWW, there has been more ambiguity to who or what is on the other side as well as their desire for others' devices. Hacking from lone wolves to nations' states is now prevalent across this new domain, and for the last 15 years, countries have used it as a statecraft for espionage and warfare.

Estonia marked the beginning of weaponizing cyberspace, but no permanent damage has been associated with this disruption. In 2010, we saw physical destruction of machines. A joint American/Israeli operation called Olympic Games used a cyber

> “
>
> ***When the WWW opened its aperture to the world, the public and private sectors became so interconnected that it is now considered by some countries as a human right.***

tool called Stuxnet to destroy Iranian nuclear centrifuges. In this operation, we saw damage in the physical world from the virtual environment [4].

In this new world order, modern militaries are seeing their networks, weapons systems, and infrastructures become vulnerable to these types of cyberattacks. Defined by the National Institute of Standards and Technology, a cyberattack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" [5].

U.S. AIR FORCE (USAF) INTEGRATED CYBER DEFENSE STRATEGY

Just like the rest of the world, the USAF learned that the cyberspace network is the backbone infrastructure for other organizations to use in creating weaponized cyberspace effects. In 2016, they started transforming their legacy communications squadrons to cyberspace operations squadrons. They called this transformation the Cyber Squadron Initiative (CSI) [6]. For example, a USAF pilot operates the aircraft but does not fix it; an aircrew member is the operator of the weapons system, not the maintainer. In the same vein, the communications squadrons are the maintainers of the network. These new cyberspace operations squadrons would become the "pilots," or operators, in this new domain. They would have to gain new trade skills and experiences, utilizing their computers as weapons inside the network. The Cyber Squadron Enabling Concept, signed in 2018, and the Program Action Directive for CSI, signed in 2020, finalized the creation of these teams and processes. The USAF created operational units called Mission Defense Teams (MDTs) to defend their interconnected assets in cyberspace. This concept was built on integrated cyber defense [7].

Integrated cyber defense is a layered model that provides three key components: proactive defense, resiliency, and defense in depth (Figure 2). Proactive defense is human cyber defenders seeing potential cyber adversaries in their communications and weapons system networks. These defenders can prevent and fight off cyber intrusions. Resiliency is the idea of building or improving these systems, or processes, during a conflict. And defense is the layered, automated, or semiautomated tools to initially block intrusions.

The foundation of this defense is placed upon the network infrastructure, called information technology (IT). Functional mission analysis cyber is a sublayer to this foundation that identifies risks and where that risk (cyber terrain) goes in the mission.

The concept and model of integrated cyber defense is solid. Combining humans and machines to defend cyberspace makes total sense when facing today's cyber challenges.

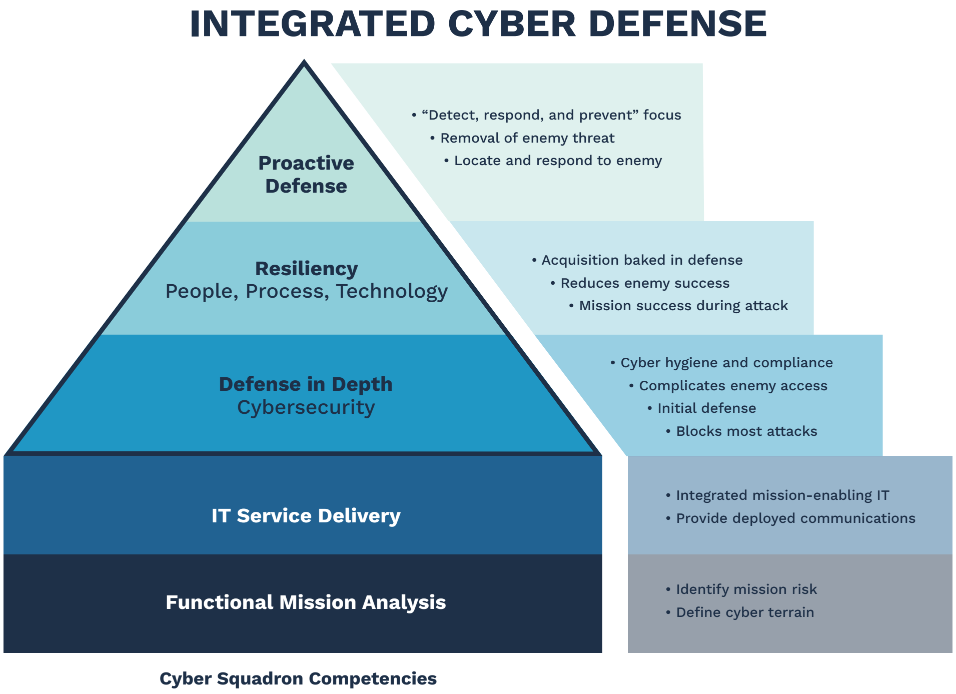

INTEGRATED CYBER DEFENSE
Proactive Defense
• "Detect, respond, and prevent" focus
• Removal of enemy threat
• Locate and respond to enemy
Resiliency
People, Process, Technology
• Acquisition baked in defense
• Reduces enemy success
• Mission success during attack
Defense in Depth
Cybersecurity
• Cyber hygiene and compliance
• Complicates enemy access
• Initial defense
• Blocks most attacks
IT Service Delivery
• Integrated mission-enabling IT
• Provide deployed communications
Functional Mission Analysis
• Identify mission risk
• Define cyber terrain
Cyber Squadron Competencies

Figure 2. Cyber Defense Layered Model *(Source: U.S. Air Force).*

> ***Combining humans and machines to defend cyberspace makes total sense when facing today's cyber challenges.***

CHALLENGES AND OPPORTUNITIES

The USAF's first challenge in its cyber defense strategy was to move the military members from communications to cyber operations. They created the MDTs to host the new cyber operations squadrons. However, people still needed to take care of the network, so they invested into Enterprise IT as a Service (EITaaS) in 2018 [8]. EITaaS is the process of contracting network maintenance out to companies, but it comes with a $6B bill.

That same year, the USAF consolidated all cyber equities to the Air Combat Command and created a three-star numbered air force called 16 Air Force (AF) a year later. The 16 AF combined intelligence and cyberspace into one area. By 2022, there were 84 MDTs across the AF bases, or wings. The USAF is the only service invested in this type of cyber defense at the base level and controlled by the base commander for their wing priorities. This year, they divested most of the teams and only funded 19 of them.

What happened? We will explore factors that possibly contributed to this in the following sections.

INTEGRATED DEFENSE MODEL

We will discuss each area of the integrated defense model and what improvements can be made to salvage it and make it a combat-effective capability for the USAF.

Proactive Defense

Proactive defense is given to the base or wing commander, a colonel most likely, who has no formal education in cyberspace and is usually a legacy operator of an aircraft or missile system. Many of these commanders do not even know they have MDTs on their bases, nor do they know how to utilize them. As a result, MDTs are not executing mission-relevant operations and are still inside their communications squadrons, residing at the mission support groups and away from the operations groups. Since support groups are there to support wing functions like computer repair or network outages, many MDT members are still doing legacy support, even with EITaaS at their bases.

MDTs are not sent to a formal training school like aircrews. When attending formal training schools, aircrews not only learn about their aircraft but how to employ that weapons system in a combat environment where multiple effects are taking place. They know where their combat capabilities fit into the larger war effort. Flying is the easy part; combat employment, in context of a highly contested environment, is the tougher skill to learn. In contrast, MDTs are getting computer-based training, which involves a few weeks of understanding cyber tools to utilize in defense and learning how to assess risk in their networks, including weapons systems and base infrastructure.

The higher command has never issued a timeline to complete training or execute first missions. Some teams have stayed in the training pipeline for years, never converting to being fully mission qualified. The return on investment of these teams to show mission effectiveness in cyber defense of a base was very low. Of the teams that showed effectiveness, the secret sauce was two-fold—wing leadership buy-in and understanding the importance of cyber defense as well as integrating these MDTs into all aspects of their base mission, including operations, maintenance, support, and intelligence. The teams met regularly with their counterparts and debriefed wing leadership on their mission status and the priorities their wing commanders gave them.

To improve their effectiveness, the MDTs must be held accountable to a timeline for mission qualification, which is the responsibility of the Air Combat Command. In addition, the Air Education and Training Command, particularly Air University, needs to offer cyber education to new wing and group commanders when all new commanders go to Maxwell Air Force Base in Montgomery, AL, for their required courses. MDTs need their own formal training unit, and when arriving at their base, they need mission qualification training for their base mission (fighter, bomber, missile systems, etc.). Integration at the wing level and into all exercises and training opportunities is necessary since all other wing units do this.

Resiliency

Resiliency is not addressed in the integrated cyber defense model. There is a complete misunderstanding of mission risk, which is defined in simple terms as a threat acting upon a vulnerability [9]. To quantify risk, there is the evaluation of consequence and the likelihood a negative event would take place. Risk assessments usually only incorporate one system or domain. However, when using system theory, mission risk pertains to a system of systems needed to operate in any complex environment, including combat. Most cyber risk assessments would showcase one area—outdated servers or unpatched computers. All servers need electricity, air conditioning, physical security, and connectivity to the computers they are interconnected with. Servers operate in a system of systems. For example, if an air conditioning unit was 20 years old, instead of updating a 3-year-old server, the air conditioner should be fixed first before the servers overheat when the unit breaks down.

Also, integrating and including the intelligence community into these risk assessments is necessary because not all vulnerabilities are acted upon. Intelligence, just like battlefield assessments of enemy missile and aircraft systems, uses this to understand weaknesses and prioritize courses of action for decision-making. Cyber defense is no different.

A better way to view cyber risk assessments is understanding the mission first and what pathways the systems utilize to execute that mission. Fusing the MDT with operations, maintenance, and intelligence when those risk assessments are being made allows risk to become mission risk; risk is now in context. Two other important risk areas involve the enemy and one's own system. For example, in cyber defense, we have learned over the years that China steals intellectual property vice Russia that disrupts allies' systems. Those are two completely different focus areas—the cyber defense teams and the tools needed to defend those networks. Knowing one's systems and which has the most vulnerabilities are key factors when performing these assessments. Cyber teams and IT professionals do not own risk. They advise on risk. Leaders and commanders own the risk. Cyber teams are there to inform and help leaders prioritize risk so the entire base can execute the missions.

> **“**
>
> ***A better way to view cyber risk assessments is understanding the mission first and what pathways the systems utilize to execute that mission.***

Defense in Depth

Defense in depth is not being optimized. The USAF is the one service that loves its technology more than its sister services. But even beyond the military, in the cyberspace domain, technology is king. Terms like artificial intelligence, quantum computing, and machine learning have taken over from yesterday's outdated lingo like zero trust and blockchain. The military uses technology to fill in its capability gaps. They should be asking, "What is the mission, what are the capabilities we need to execute that mission, and can technology answer these gaps in mission execution?" This is the starting point when finding technology that works for mission relevancy.

Retired AF Colonel Tony Franks once heard an AF general say to blockchain the entire Air Force [10]. This is probably not feasible because blockchain is a distributed database utilizing ledgers and timing, so one cannot easily manipulate a tasking [11].

However, when time is of the essence, like that involving nuclear weapons or combat search and rescue of a downed aircrew member, there should not be a delay in executing these missions for national security. On the other hand, acquisitions, lifecycle management of systems, and contracting can be blockchained. We should use the right tool for the job—the right technology for the mission requirements.

Beyond technology are people. Knowing the enemy is critical, but knowing the people is more important. Cybersecurity is vital to our missions in the military, and industry has handled it through automated and semi-automated defenses and tools. There have been more cybersecurity violations from negligent users than any enemy lurking in the cyber shadows. We need to increase, improve, and update our cybersecurity training in the services. Education is the cheapest way to defend ourselves in this domain. Because leaders have different training and education needs than their subordinates, airmen should have multiple training venues that take them on a cybersecurity journey through their entire career, from basic cyber hygiene to advanced awareness and tactics. In addition, members of a wing should get classified briefings on enemy cyber capabilities and their own weapons system vulnerabilities.

CONCLUSIONS

The USAF should be the most lethal airpower component in the world. This world is completely interconnected in cyberspace, and cyber defense is an incredible challenge. The old world saw that a good defense could always outlast an invading army. In this new world order, cyber offense just needs a single avenue to get through a layered cyber defense. There will never be a perfect cyber defense, but we should not make it easy for the enemy. The goal of the AF Integrated Cyber Defense Strategy should be to make adversarial cyber intrusions so difficult and expensive to conduct that the adversary does not want to attack due to the combat cost. Addressing these challenges, we can implement that strategy effectively for our nation. ■

NOTE

This article is the opinion of the author and does not represent the views of the U.S. government, USAF, or Air University.

REFERENCES

[1] Ottis, R. "Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective." Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, pp. 163–168, 2008.

[2] NPR. "30 Years Ago, One Decision Altered the Course of our Connected World." https://www.npr.org/2023/04/30/1172276538/world-wide-web-internet-anniversary, accessed 17 July 2023.

[3] DARPA. "ARPANET." https://www.darpa.mil/about-us/timeline/arpanet, accessed on 17 July 2023.

[4] CSO. "Stuxnet Explained: The First Known Cyberweapon." https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html, accessed on 17 July 2023.

[5] NIST. "Cyberattack." https://csrc.nist.gov/glossary/term/Cyber_Attack#term-def-text-1, accessed on 17 July 2023.

[6] USAF. "Cyber Squadron Initiative: Arming Airmen for 21st Century Battle." https://www.af.mil/News/Article-Display/Article/1174583/cyber-squadron-initiative-arming-airmen-for-21st-century-battle/, accessed on 17 July 2023.

[7] USAF Headquarters. "Cyber Squadron Initiative." https://www.dafitc.com/wp-content/uploads/Cyber-Squadron-Initiative.pdf, August 2018.

[8] USAF Materiel Command. "ETIaaS Wave 1 Services Awarded in $5.7B Agreement." https://www.afmc.af.mil/News/Article-Display/Article/3377827/eitaas-wave-1-services-awarded-in-57b-agreement/, accessed on 17 July 2023.

[9] Washington University St. Louis. "Vulnerabilities, Threats, and Risks Explained." https://informationsecurity.wustl.edu/vulnerabilities-threats-and-risks-explained/, accessed on 17 July 2023.

[10] Franks, T. Personal communication. AF Center for Strategy and Technology, 31 August 2023.

[11] Investopedia. "Blockchain Facts: What Is It, How It Works, and How It Can Be Used." https://www.investopedia.com/terms/b/blockchain.asp, accessed on 17 July 2023.

BIOGRAPHY

ANTHONY FRANKS is an Air University professor who teaches at the Chief of Staff of the AF's academic fellowship, Blue Horizons, where he educates battle-ready entrepreneurs capable of leading positive, disruptive change by creating and testing prototypes for combat viability. His focus areas are military cyber operations, special operations in grey zone warfare, and joint military warfare. He served 24 years in the USAF as a pilot and cyberspace operations officer and taught cyber operations education for five years at the USAF Cyber College. Col. Franks holds a B.S. in business management, an M.A. in military strategy, and an M.S. in theology.

DARK NET

USAGE FOR COUNTRIES IN CONFLICT

BY KEVEN HENDRICKS (PHOTO SOURCE: CANVA)

INTRODUCTION

For many, the "dark web" harbors a stigma. After the rise of notorious "dark net markets" like "Silk Road" and "AlphaBay" in the early 2010s, pop culture has come to equate the "dark web" with illegality and contraband. Something often forgotten and the altruistic cornerstone as to why the dark web exists in the first place is the mitigation of internet censorship. The dark web is a medium for those to access information and communicate in a censorship-resistant environment. It is imperative for U.S. Department of Defense partners to understand dark web intelligence is a crucial component of the open-source intelligence discipline, especially for countries in conflict.

Because of freedom of speech and freedom of press, America is naive when it comes to internet censorship. Many countries throughout the world heavily censor the internet for their citizens and completely control what content the populus can view. It is estimated that 5.18 billion people utilize the internet, equated to 64.6% of the world's population as of April 2023 [1], for countless purposes—from news/information to social media to entertainment. Of those 5.18 billion users, how many are throttled by their governments as to what they are allowed to do when they go online?

> ***The altruistic cornerstone as to why the dark web exists in the first place is the mitigation of internet censorship.***

A January 2023 article published by Comparitech [2] rated the various countries throughout the world that strictly control the internet for their citizens. North Korea and China possessed the most internet censorship. Furthermore, the commonality of heavy internet censorship coinciding with totalitarian regimes/dictatorships is unremarkable. From this, how does internal and external conflict in a country correlate to internet censorship and, by extension, the means to circumvent those protocols? How does dark web usage or virtual private network (VPN) connectivity to peer-to-peer facilitated "mesh nets" directly impact war or civil unrest?

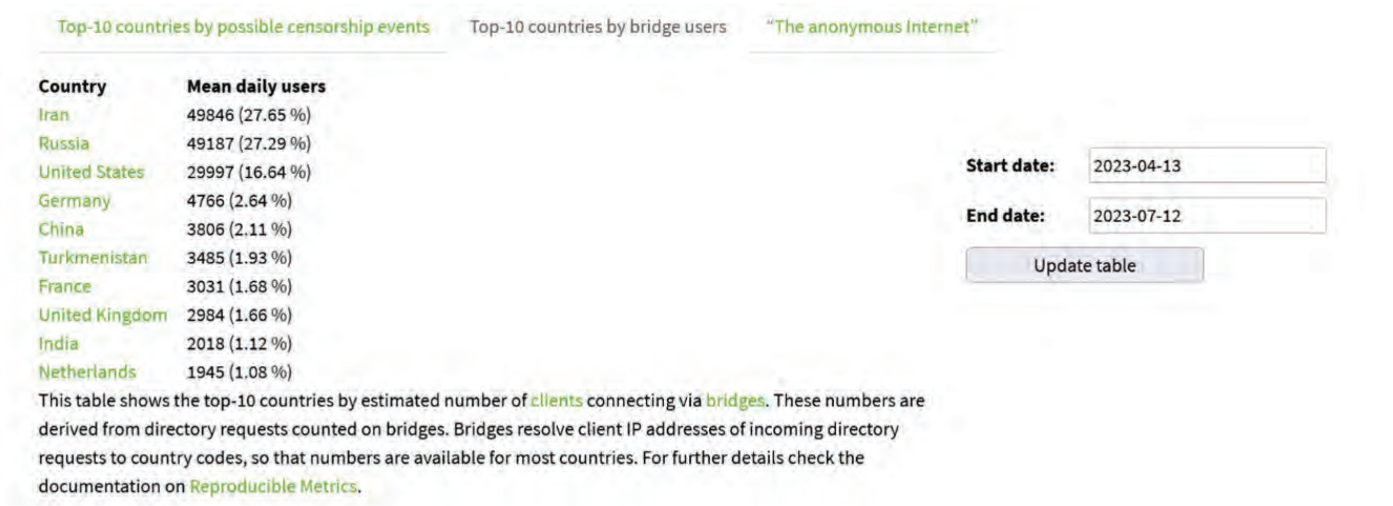
THE DARK WEB DURING THE RUSSIA-UKRAINE WAR

The ongoing conflict between Ukraine and Russia has surpassed a year. In August 2022, *The New Statesman* published an article about how the Russian invasion in Ukraine was "reshaping the dark web" and that "the geopolitical tensions that have changed the world are also changing the dark web" [3]. Although this article was published during the first six months of the Russia-Ukraine conflict, the perception of geopolitical tensions transcending to the dark web is apparent.

While the dark web is often shrouded with anonymity, individual "dark nets" are often very transparent in the metrics concerning the scope of their usage. For example, global privacy service Tor offers its metrics via the Tor Project, where multiple components of the network can be viewed (Tables 1 and 2).

Russia started tightening its restrictions on VPN services like Tor and dark web usage two months before the invasion of Ukraine, in December 2021. In an article published that same month, Reuters highlighted the "crackdown," where

Table 1. Top 10 Countries by Bridge Users April 2023 – July 2023 *(Source: Tor Metrics [4])*


Top-10 countries by possible censorship events
Top-10 countries by bridge users
"The anonymous Internet"
Update table

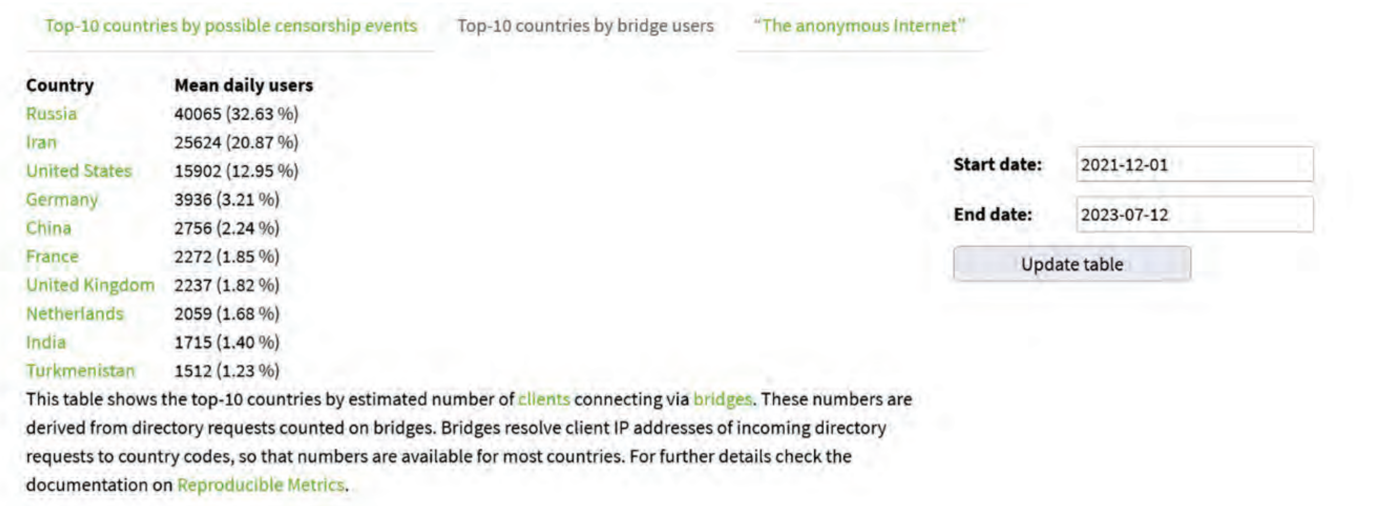
Country	Mean daily users
Iran	49846 (27.65 %)
Russia	49187 (27.29 %)
United States	29997 (16.64 %)
Germany	4766 (2.64 %)
China	3806 (2.11 %)
Turkmenistan	3485 (1.93 %)
France	3031 (1.68 %)
United Kingdom	2984 (1.66 %)
India	2018 (1.12 %)
Netherlands	1945 (1.08 %)

Start date: 2023-04-13

End date: 2023-07-12

This table shows the top-10 countries by estimated number of clients connecting via bridges. These numbers are derived from directory requests counted on bridges. Bridges resolve client IP addresses of incoming directory requests to country codes, so that numbers are available for most countries. For further details check the documentation on Reproducible Metrics.

Table 2. Top 10 Countries by Bridge Users December 2021 – July 2023 *(Source: Tor Metrics [4])*


Top-10 countries by possible censorship events
Top-10 countries by bridge users
"The anonymous Internet"
Update table

Country	Mean daily users
Russia	40065 (32.63 %)
Iran	25624 (20.87 %)
United States	15902 (12.95 %)
Germany	3936 (3.21 %)
China	2756 (2.24 %)
France	2272 (1.85 %)
United Kingdom	2237 (1.82 %)
Netherlands	2059 (1.68 %)
India	1715 (1.40 %)
Turkmenistan	1512 (1.23 %)

Start date: 2021-12-01

End date: 2023-07-12

This table shows the top-10 countries by estimated number of clients connecting via bridges. These numbers are derived from directory requests counted on bridges. Bridges resolve client IP addresses of incoming directory requests to country codes, so that numbers are available for most countries. For further details check the documentation on Reproducible Metrics.

the Russian government blocked access to the Torproject.org, a climax in a multiple year campaign of enforcing restrictions for VPNs [5].

Conversely in February of 2023, Russia elicited the dark net market's "BlackSprut" for a paid billboard advertisement displayed in Moscow. CybersecurityConnect described this move as follows [6]:

> The important question is how the advertisement made it onto the billboard in the first place. It could be a hacked device, or an innocent oversight from the billboard's operator, but there's no denying that Russia is a far friendlier place for darknet markets to operate than many countries. That the country is profiting from a wide range of crypto transactions to get around strict sanctions placed upon the country following its illegal invasion of Ukraine could also be a factor. And it doesn't hurt that, reportedly, the operators of the market support Russia's war and have even gone so far as to support Russian-allied troops with crypto donations.

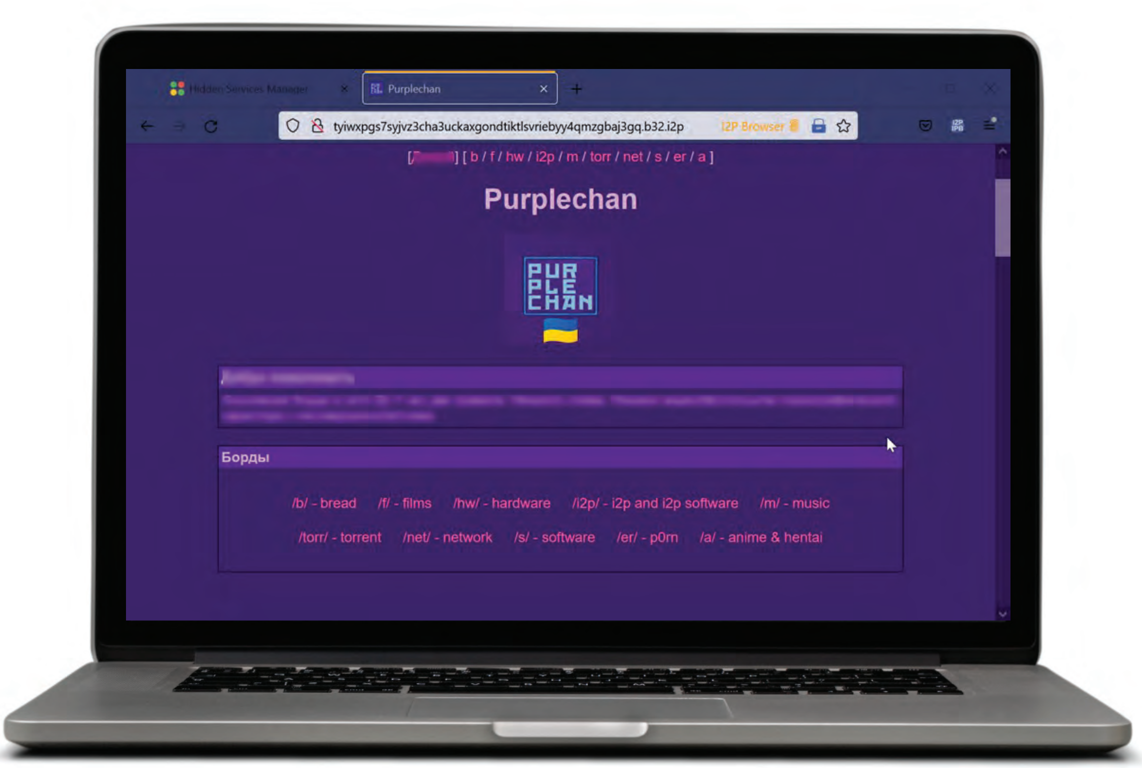
PHONE APPS DURING THE RUSSIA-UKRAINE WAR

Another development with dark web usage germane to Russia was the rise of mobile phone apps for individual dark net markets juxtapose the traditional dark web browser usership (Tor, I2P, etc. [7]) (Figure 1). As the conflict between Russia and Ukraine neared its one-year anniversary, a DeviceSecurity.io article highlighted the recent rising trend of Russia eliciting dark net markets for mobile app connectivity for its customers [8]. The ease of use with market-specific apps built for Android operating systems allowed ready access to Russian markets like "RuTor," "Blacksprut, and "OMG!OMG!"

> **66**
>
> ***Another development with dark web usage germane to Russia was the rise of mobile phone apps for individual dark net markets.***

Inasmuch, the events that unfolded in the months leading to the one-year anniversary of the Russia-Ukraine conflict beckons the question as to why Russia seemingly laxed its stranglehold on Tor/VPN usage. As highlighted in the CybersecurityConnect article [6], could the illicit cryptocurrency economy derived from the various dark net markets result in an influx of pro-Russia donations from those market administrators? Could this "passive income" circumvent international sanctions and subsidize Russian military aggression? Could the Russian government want to keep its population appeased by turning a blind eye to the illicit activity with a dark web nexus? Could the increase in dark web usage, more specifically Tor, simply be state-sponsored cyberwarfare vs. the general population?

According to the Tor Metrics data in Tables 1 and 2, Russia has accounted for upward of 20% to 35% of the bridge users by country since December 2021, when Moscow tightened the dark web/VPN restrictions. However, according to the same data, over the past year, another country ripe with internal conflict and social unrest has taken over as the top country for bridge users—Iran.



tyiwxpgs7syjvz3cha3uckaxgondtiktlsvriebyy4qmzgbaj3gq.b32.i2p

[/[redacted]] [b / f / hw / i2p / m / torr / net / s / er / a]

Purplechan

[redacted]

Борды

/b/ - bread /f/ - films /hw/ - hardware /i2p/ - i2p and i2p software /m/ - music

/torr/ - torrent /net/ - network /s/ - software /er/ - p0rn /a/ - anime & hentai

Figure 1. Pro-Ukraine i2P Forum "PurpleChan" *(Source: i2p Forum [7]).*

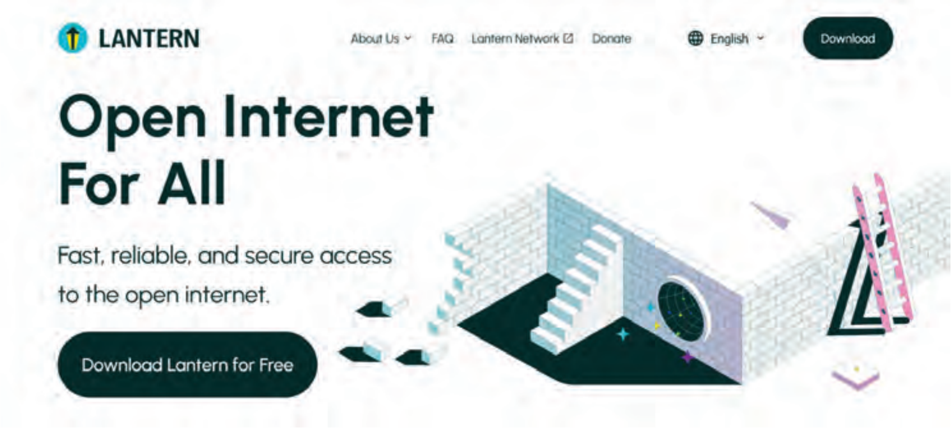
THE DARK WEB IN IRAN

Iran is a country that has a unique relationship with the dark web. They have very successful cyber criminals and ransomware groups with no affiliation to the Islamic Revolutionary Guard Corps, like SamSam actors, and state-sponsored cyber espionage and hacking groups known as advanced persistent threats. Iran is also a country that restricts dark web usage for its citizens and often completely turns off their internet during heightened periods of civil discourse, as highlighted in a *WIRED* magazine article that described when the nationwide protest and vision clashes with the government sparked a five-day internet shutdown on November 15, 2019 [9].

For a populous that has grown accustomed to such authoritarian practices as well as highly publicized events, it is no surprise that when the Mahsa Amini protests began in September 2022, many rushed to aid the inevitable forthcoming internet "lockdown." One month after the protests began, CNBC reported such hacking conglomerates as "Anonymous" were conducting cyberattacks on the Iranian government infrastructure [10].

One VPN service that has spearheaded the campaign for internet freedom in Iran is Lantern VPN (Figure 2). However, the Oxen Privacy Tech Foundation (OPTF), which developed the "LokiNet" dark net as well as the end-to-end encryption messenger "Session," saw an overwhelming influx of Iranian users since September 2022. The OPTF worked diligently to incorporate the support Persian (Farsi) script into the Session service and support connectivity from various VPNs circumventing Iranian firewalls (Figure 3).

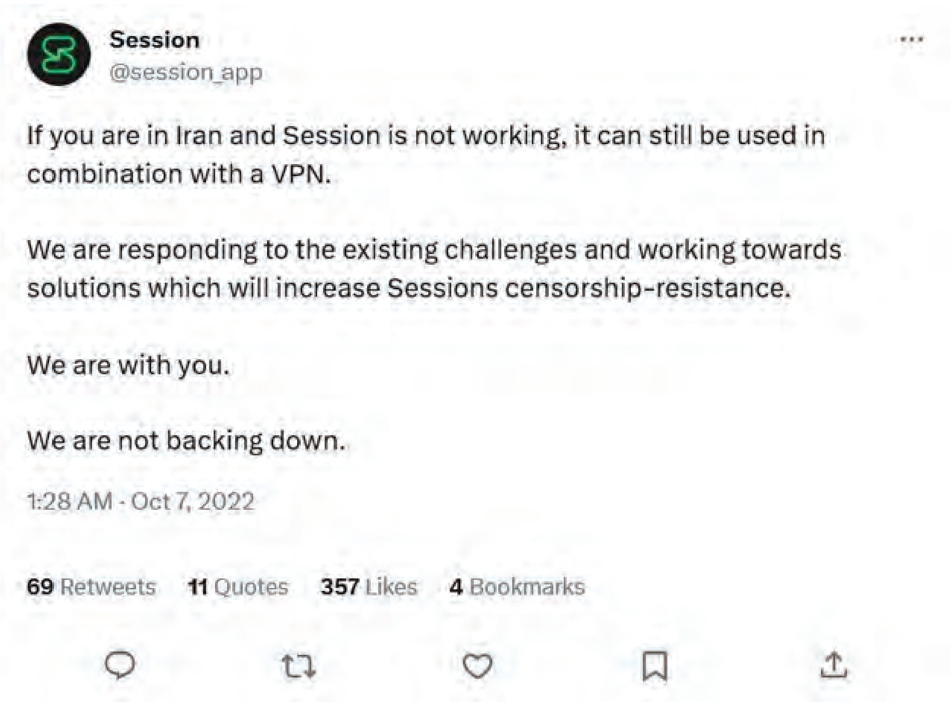
While Iran's extreme tactics carry much notoriety, internet censorship is well known in many countries throughout the Arabian Peninsula. Many human rights and free press organizations have a presence on various dark nets. An example can be seen in Figure 4, where Saudi Arabia Human Rights campaign group ALQST hosted on I2P to sidestep the governmental firewalls.



Open Internet For All

Fast, reliable, and secure access to the open internet.

Figure 2. Lantern VPN for Iran *(Source: Lantern [11]).*



Session
@session_app

If you are in Iran and Session is not working, it can still be used in combination with a VPN.

We are responding to the existing challenges and working towards solutions which will increase Sessions censorship-resistance.

We are with you.

We are not backing down.

1:28 AM · Oct 7, 2022

69 Retweets 11 Quotes 357 Likes 4 Bookmarks

Figure 3. Session Script on X/Twitter *(Source: Session [12]).*

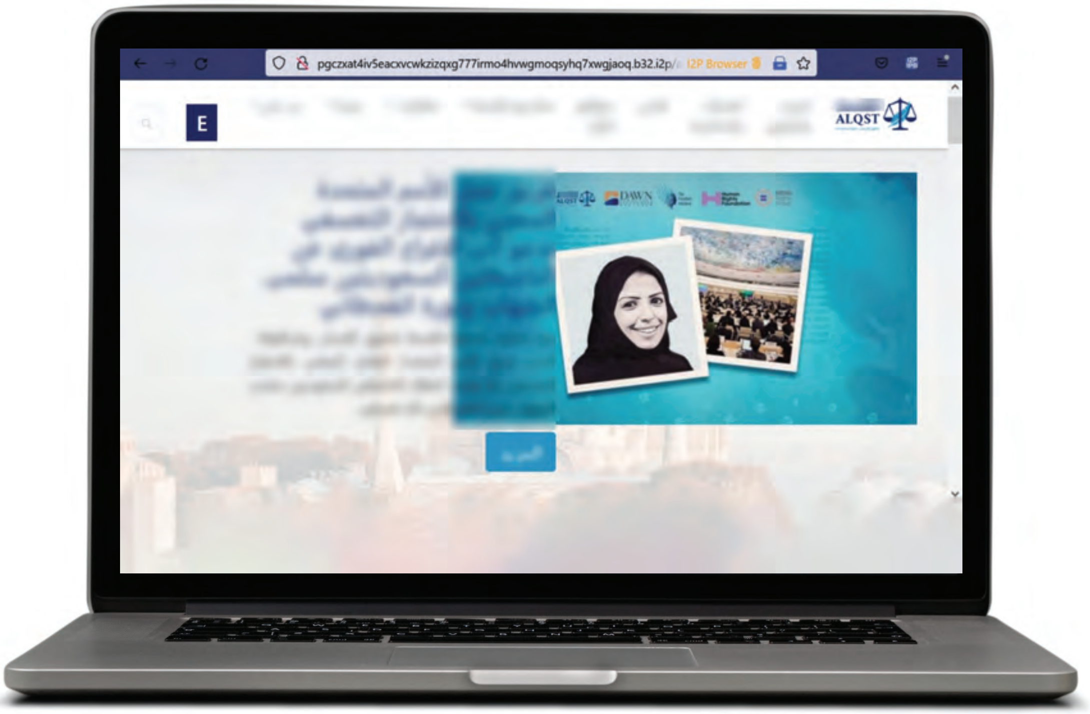

pgczxat4iv5eacxvcwkzizqxg777irmo4hvwgmoqsyhq7xwgjaoq.b32.i2p/
I2P Browser
E
ALQST
DAWN

Figure 4. Saudi Arabia Human Rights Organization ALQST "Eepsite" *(Source: ALQST for Human Rights [13]).*

CONCLUSIONS

With the events unfolding across Europe or in the Middle East, the dark web remains an essential component to empower internet freedom for those engulfed in the turmoil. For many in the United States, it merely remains a novelty—a gateway into a shadowy underworld where contraband and taboo reign supreme. It is something we are quick to portray in pop culture with many negative connotations. For those who are enveloped within country conflicts and severely restricted from what they can view or say online, the dark web serves as the only avenue to communicate or see the outside world. Gathering intelligence from its sources is a critical process to understanding social sentiments and developing trends within war-torn regions. ■

> ***With the events unfolding across Europe or in the Middle East, the dark web remains an essential component to empower internet freedom for those engulfed in the turmoil.***

REFERENCES

[1] Statista. "Number of Internet and Social Media Users Worldwide as of April 2023." https://www.statista.com/statistics/617136/digital-population-worldwide/, accessed on 29 august 2023.

[2] Comparitech. "Internet Censorship 2023: A Global Map of Internet Restrictions." https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/, accessed on 29 August 2023.

[3] Grunewald, Z. "How the War in Ukraine Is Reshaping the Dark Web." *The New Statesman*, https://www.newstatesman.com/spotlight/tech-regulation/cybersecurity/2022/08/ukraine-war-cyber-attacks-the-dark-web, accessed on 29 August 2023.

[4] Tor Metrics. https://metrics.torproject.org, accessed on 29 August 2023.

[5] Reuters. "Russia Blocks Privacy Service Tor, Ratcheting Up Internet Control." https://www.reuters.com/technology/russia-ratchets-up-internet-crackdown-with-block-privacy-service-tor-2021-12-08/, accessed on 29 August 2023.

[6] CyberSecurity Connect. "Russian Dark Web Market Advertises Itself on Moscow Billboard, While Donating to Russian Troops." https://www.cybersecurityconnect.com.au/defence/8678-russian-darkweb-market-advertises-itself-on-moscow-billboard-while-donating-to-russian-troops, accessed on 29 August 2023.

[7] i2p Forum. "PurpleChan." http://purplechan.i2p, accessed on 29 August 2023.

[8] DeviceSecurity.io. "Darknet Markets Using Custom Android Apps for Fulfillment." https://www.devicesecurity.io/blogs/darknet-markets-using-custom-android-apps-for-fulfillment-p-3351, accessed on 29 August 2023.

[9] WIRED. "The Dark Web, Iran Style." https://wired.me/technology/iran-dark-web-internet-blackout/, accessed on 29 August 2023.

[10] CNBC. "Hacktivists Seek to Aid Iran Protests With Cyberattacks and Tips on How to Bypass Internet Censorship." https://www.cnbc.com/2022/10/05/how-anonymous-and-other-hacking-groups-are-aiding-protests-in-iran.html, accessed on 29 August 2023.

[11] Lantern. "HomePage." https://lantern.io, accessed on 29 August 2023.

[12] Session. https://twitter.com/session_app/status/1578255877429022721?lang=en, accessed on 29 August 2023.

[13] ALQST for Human Rights. "Eepsite." http://alqst.i2p, accessed on 29 August 2023.

BIOGRAPHY

KEVEN HENDRICKS is a 16-year veteran detective with a municipal police department and has served as a task force officer for two separate federal agencies. He is a published author with the *FBI Law Enforcement Bulletin* and *American Police Beat* and currently works as an instructor for Street Cop Training and Noble Supply & Logistics, teaching a class for law enforcement on dark web and cybercrime investigations. He is a certified cybercrime examiner and cybercrime investigator by the National White Collar Crime Center, a certified cryptocurrency investigator through the Blockchain Intelligence Group, and a certified digital asset professional through the Global Digital Asset & Cryptocurrency Alliance.

CSIAC Cybersecurity & Information Systems Information Analysis Center

TECHNICAL INQUIRY SERVICES

FOUR FREE HOURS

Research within our four focus areas available to academia, industry, and other government agencies. Log in to csiac.org to submit your inquiry today.

TECHNICAL AREAS

Cybersecurity

Knowledge Management & Information Sharing

Modeling & Simulation

Software Data & Analysis

Photo Source:
U.S. Air Force and 123.com

A DEFENSE-IN-DEPTH AND LAYERED APPROACH TO SOFTWARE SUPPLY CHAIN SECURITY

ABDUL RAHMAN (PHOTO SOURCE: 123RF.COM)

SUMMARY

In this article, we will discuss the confluence and utility of using software supply chain (SSC)-focused frameworks (The Updated Framework [TUF] and the in-toto framework), combined with behavioral approaches using artificial intelligence (AI) aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), to generate a truly comprehensive approach for SSC security [1]. Such a "defense-in-depth" approach recognizes that these frameworks by themselves fall short of addressing the guidelines for the integrity of SSCs. We will also examine the common attacks currently employed against SSCs and how both frameworks can be utilized to prevent such attacks, along with suggestive alignment with required compliance frameworks [1–3].

TABLE OF CONTENTS

Additionally, we will explore the possibilities, challenges, best practices, benefits, and potential uses of AI computing models to assure the security of high-value SSCs. Of all the potential uses of emerging AI-enabled and machine-learning (ML) tools to promote cybersecurity in the defense community, their application to protecting software supply chains may be one of the most promising given the massive volume of coding information involved [4]. The U.S. Department of Defense's (DoD's) Chief Digital and Artificial Intelligence Office (CDAO), which the department recently established in June 2022, is already seeking to use AI and ML tools to conduct analysis within digital engineering and cyber supply chain use cases [5].

Because the success of an AI/ML tool depends, in part, on acquiring useful data in a timely manner, curating stored data plays a central role in producing high-efficacy predictions. Reasoning over these features drives recommendations for optimizations, leading to improvements in overall SSC security. This includes identifying the following:

- Potential software-build bottlenecks (inclusive of on-premise, cloud, and hybrid),
- Usage trends,
- Vulnerabilities aligned with using libraries (e.g., dynamic link libraries, portable executables, etc.), and
- Fraudulent actions.

To protect critical military and homeland security SSCs, AI/ML-based supply chain analysis can be trained on a broad set of local, distributed, network, and end-point data to infer the probability of security threats and vulnerabilities in the supply chain.

BACKGROUND

An SSC refers to a collection of software modules, libraries, and components built by third parties and the processes involved in developing and assembling software distributions. One leading software developer notes that an SSC includes all "networks of information about the software," including its hardware, operating systems, and cloud services; the software's sources "like registries, GitHub repositories, codebases, or other open-source projects"; and even the people who write its code [6]. Today's enterprise software products are intentionally engineered to draw upon broad software communities to enable more efficient, familiar, and interoperable baselines. Developers achieve this by leveraging code sourced from external (but interconnected) libraries and modules that may serve different purposes for an application (e.g., encryption, authentication, and networking).

Although efficiencies are gained through this form of community development, it also presents numerous opportunities for introducing harmful vulnerabilities and weaknesses, as an entity that acquires such software has limited visibility into and surety of the build's security [2]. Specifically, admitting dependencies through SSC development processes facilitates exploitable software code that can yield numerous (and cascading) vulnerabilities into the postbuilt product code baseline (see Figure 1). As a result, the security of an application's SSC is crucial to ensure that the final software product remains free from malicious elements like backdoors (whether "hidden" or unintentionally built) or other vulnerabilities. A compromised SSC can have a widespread impact, as it will most likely affect multiple users simultaneously.

The "SolarWinds" cyberattack levied in 2020 against multiple U.S. federal government systems by foreign adversarial groups precisely exploited these types of shortcomings in software supply chain security [7, 8]. In what the U.S. Government Accountability Office (GAO) has called "one of the most widespread and sophisticated hacking campaigns

> ***The security of an application's SSC is crucial to ensure that the final software product remains free from malicious elements like backdoors.***

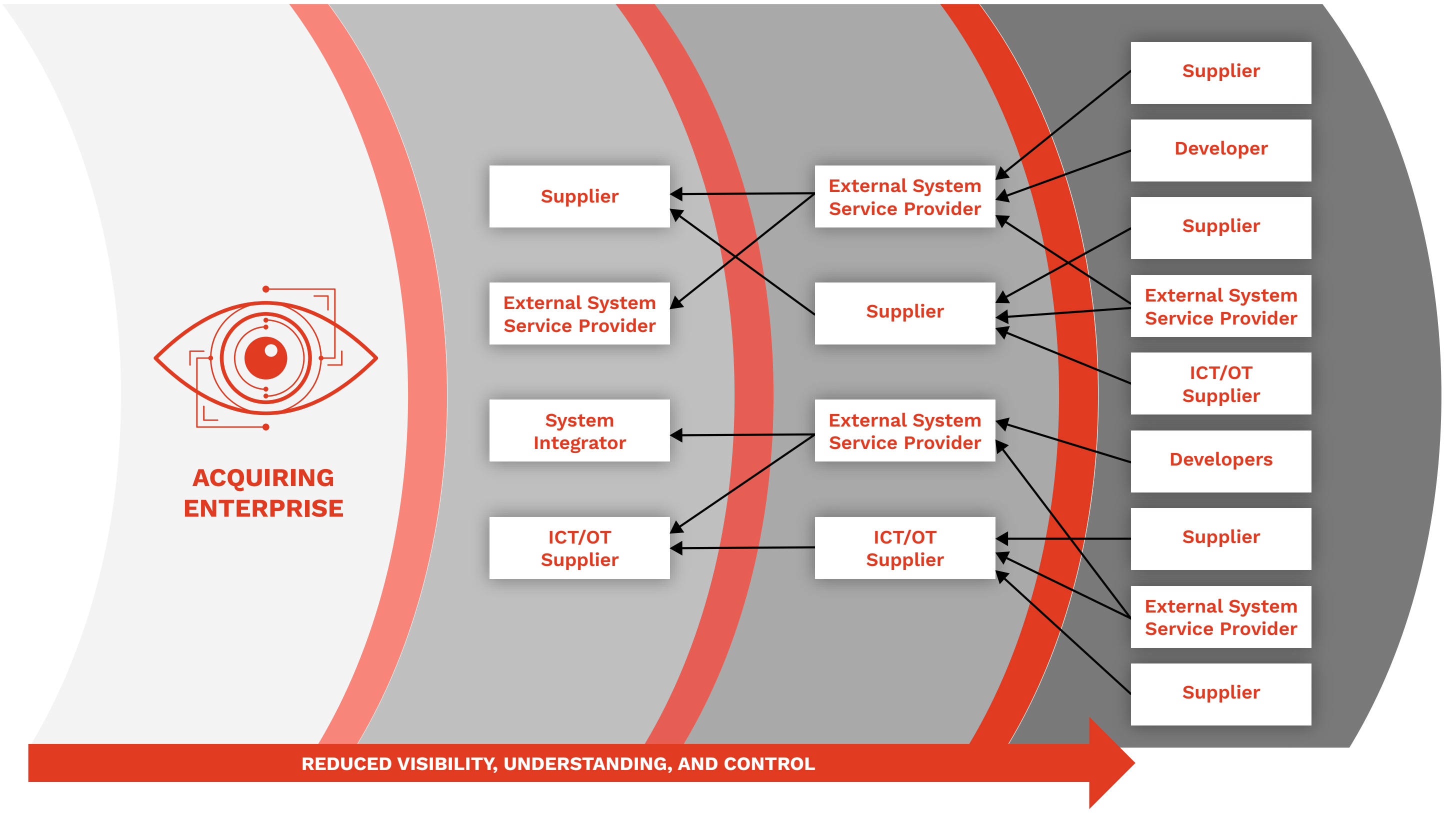

ACQUIRING ENTERPRISE
Supplier
External System Service Provider
System Integrator
ICT/OT Supplier
External System Service Provider
Supplier
External System Service Provider
ICT/OT Supplier
Supplier
Developer
Supplier
External System Service Provider
ICT/OT Supplier
Developers
Supplier
External System Service Provider
Supplier
REDUCED VISIBILITY, UNDERSTANDING, AND CONTROL

Figure 1. An Enterprise's Visibility, Understanding, and Control of Its SSC Decreases With Each Layer of the Broader Development Community's Involvement *(Source: NIST [2]).*

ever conducted against the federal government and private sector" [9], a threat actor compromised SolarWinds' "Orion" information technology administration suite by injecting malicious backdoor code into a routine software update package (see Figure 2). The threat actor, later identified by the intelligence community as the Russian Foreign Intelligence Service, was able to monitor affected systems, scrape information, and alter "command and control" activities. Even worse, the SolarWinds compromise went undetected for nearly 12 months [9].

SSCs are integral to applications and systems widely used across the private and public sector, and securing them from hacking or adversarial intrusion is a critical national security objective. For example, the U.S. "National Cybersecurity Strategy Implementation Plan," released in July 2023, details several federal initiatives to mitigate the risks to both public and private sector SSCs by making the digital ecosystem more "transparent, secure, resilient, and trustworthy" [10]. In part, these actions seek to increase trust in international software suppliers by requiring that federal entities and contractors follow cybersecurity supply chain risk management (C-SCRM) best practices.

The DoD is similarly focused on protecting military-specific SSCs. The Office of the Assistant Secretary of Defense for Sustainment (OASD[S]) recently listed the identification of SSC cyber vulnerabilities as one of its key activities in promoting acquisition security and is documenting existing source code exposures among the U.S. defense industrial bases [11]. The Office of the DoD Chief Information Officer is also working to finalize an enterprise-wide strategy for cyber supply chain risk management to guide protective actions for SSCs across the DoD [12].

An attack on an SSC occurs when malicious actors gain unauthorized access to and modify software at any point within the intricate software development supply chain, like what happened with the SolarWinds event. By introducing their own malicious

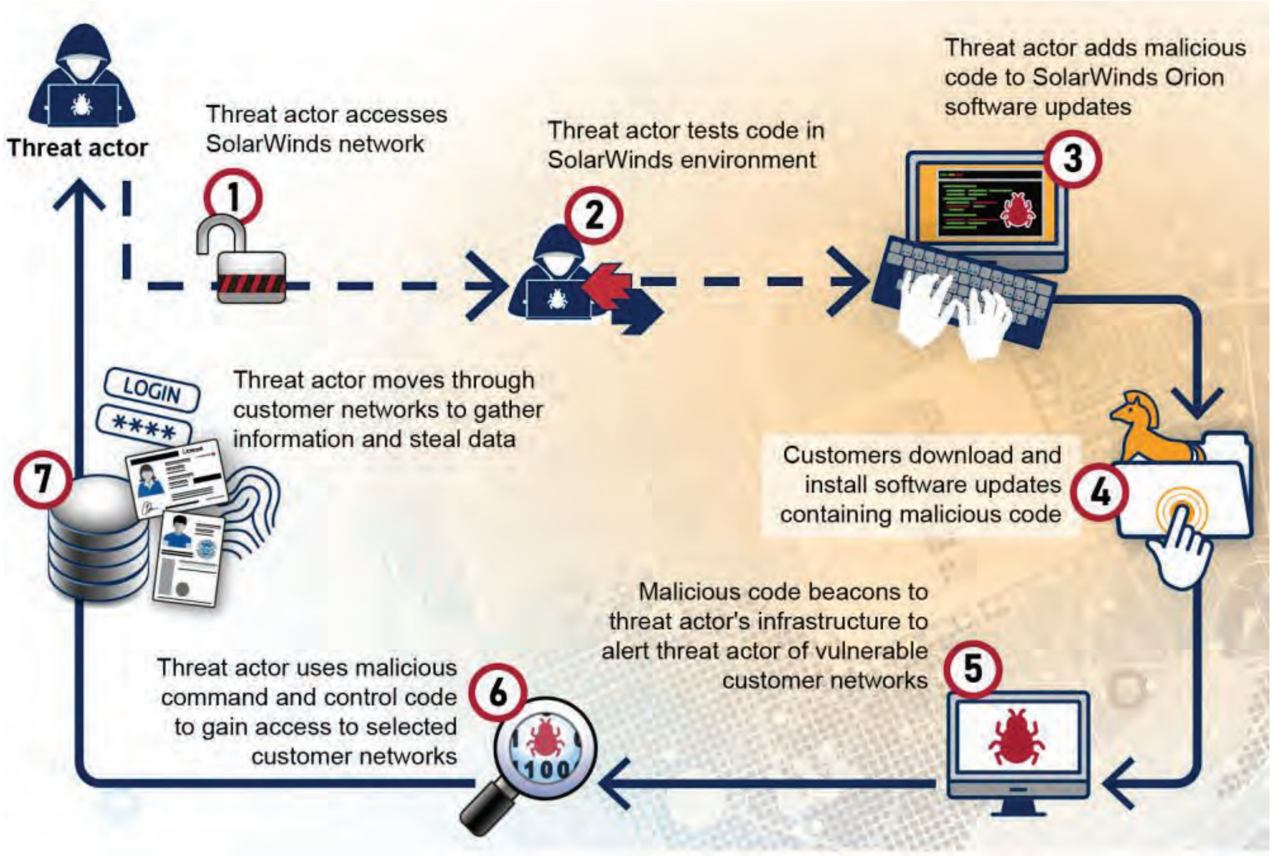

Threat actor
Threat actor accesses SolarWinds network
1
Threat actor tests code in SolarWinds environment
2
Threat actor adds malicious code to SolarWinds Orion software updates
3
Customers download and install software updates containing malicious code
4
Malicious code beacons to threat actor's infrastructure to alert threat actor of vulnerable customer networks
5
Threat actor uses malicious command and control code to gain access to selected customer networks
6
100
Threat actor moves through customer networks to gather information and steal data
7
LOGIN
****

Figure 2. GAO Depiction of How a Threat Actor Exploited SolarWinds' Orion Software in 2010 *(Source: U.S. GAO [9]).*

code, attackers aim to compromise a downstream target within the same supply chain [13]. Taking immediate action to secure SSCs—actions above and beyond the base updating of risk management plans—is necessary to effectively mitigate the risks posed by adversarial groups to both U.S. government and military network operations within this well-funded and active landscape.

INTRODUCTION

Because current government policy guidance for supply chain risk management practice can best be characterized as broad and nonspecific [14], organizations whose SSCs are the targets of advanced persistent threats (APTs) or nation-state-supported actors require more robust guidance for addressing their vulnerabilities than typically offered (see Figure 3). Due to the complexity and diversity of exploits that threaten SSCs, cybersecurity guidance would benefit greatly from identifying actionable critical details that organizations can take to directly address SSC hardening. For example, C-SCRM practices presume that organizational maturity around SSC security exists. However, suggested organizational governance and action plans (e.g., an organizational SCRM plan) generally only loosely address the direction needed for the effective triage, mitigation, and remediation of the SSC vulnerabilities that lie at the heart of SSC exploitations [14].

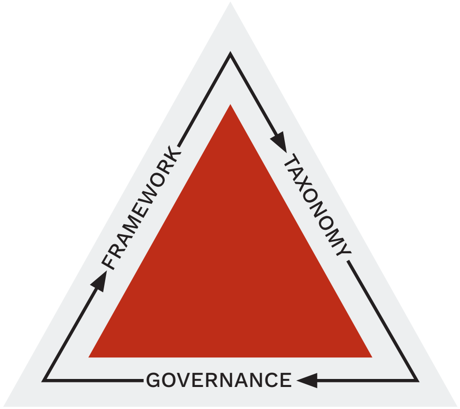


Figure 3. Project Approach for Supply Chain Risk Management Practices *(Source: U.S. DoD [11]).*

Recent data presented by Herr [13] at the USENIX Enigma conference in February 2021 suggest that SSC attacks comprise a growing set of trends that include more attacks from state actors (Russia and China) involving many of the common open-source projects used as dependencies within large organizations' SSCs. Compromising software provided by developer tools available within popular app stores is a more efficient (cost and time) method for exploiting organizations; this path currently represents 25% of documented SSC security incidents. Injecting vulnerabilities, backdoors, and software exploits into software staged within public, open-source repositories forms another 26% of attacks on SSCs, sourced from software updates to include common package management tools [15]. Common package management tools targeted by bad actors for SSC attacks can include application updaters (e.g., the FireFox browser updater), library package managers (e.g., RubyGems, PHP composure, and PIP install PyPI), and system package managers (e.g., APTs, YUM, and YaST).

> ***Compromising software provided by developer tools available within popular app stores is a more efficient (cost and time) method for exploiting organizations.***

Securing SSCs requires adopting preventive strategies against potential attacks. This can be achieved by building a baseline and engaging in robust behavioral continuous monitoring practices. These behavior-based methods involve employing AI models to forecast, infer, predict, correlate, and specify likely weaknesses, avenues of approach, and attack vectors within SSC-embedded software. Within the NIST Cybersecurity Framework (CSF), five subcategories of actions within the "Supply Chain Risk Management" category (ID.SC) of the "Identify" function lay out the key minimum or baseline actions needed for C-SCRM and are mandatory for select federal agencies (see Table 1) [1].

Including AI into C-SCRM best practices can amplify the use of existing frameworks claiming to provide "last mile" security to detect vulnerabilities already present in compromised SSCs. For example, TUF states that a software update system is only truly considered "secure" if it promptly recognizes the latest available updates, ensures the correct file downloads, and prevents any harm resulting from checking or downloading files [16]. However, TUF also acknowledges the possibility that a package could be compromised even before it reaches a software update repository.

CHALLENGES IN SSC SECURITY

Due to the complex and diverse supply chain within the U.S. government, its reliance on a vast and diverse network of suppliers and vendors for software components introduces a spectrum of challenges in securing the software components it employs. Addressing SSC challenges requires a combination of technical solutions, robust security practices, collaboration among stakeholders, and adherence to industry standards. It is crucial for organizations to prioritize SSC security to mitigate risks and protect against potential vulnerabilities and attacks. Federal entities sometimes lack complete visibility into their SSCs, including the origin, integrity, and security of components. This lack of visibility makes it challenging to identify and mitigate potential risks and vulnerabilities. In addition, relying on third-party vendors introduces risks in terms of the security practices and integrity of the software components provided.

The challenge lies in ensuring that these vendors adhere to strict security standards and supply secure software. A key weakness is the continued dependence on legacy systems and outdated software, much of it yet to be migrated or updated to newer, safer systems. These systems often have known vulnerabilities or lack necessary security updates, making

Table 1. NIST Guidance for Organizational Supply Chain Risk Management Under the "Identify" Function of the NIST Cybersecurity Framework *(Source: NIST [1])*

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	**CIS CSC 4** **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

TABLE OF CONTENTS

them attractive targets for attackers. NIST CSF, C-SCRM, and Risk Management Framework (RMF) suggest controls and compliance requirements that manifest add complexity to SSC security [1–3). Meeting these requirements while ensuring the security and integrity of the supply chain can be challenging and very manually resource intensive. Finally, workforce challenges like organizational resource constraints and a shortage of cybersecurity expertise make it difficult to effectively manage and secure the SSC. This can impede the implementation of robust security measures and practices.

SSC THREATS

Organizations and agencies in the United States should remain vigilant by implementing robust security measures, conducting regular risk assessments, and staying informed about emerging threats and attack vectors targeting SSCs. Both nation-state actors and APTs possess advanced capabilities and focus on developing aggressive, offensive cyberattack campaigns targeting the SSCs of U.S. organizations and government entities to gain unauthorized access, conduct espionage, or disrupt critical systems. These actors, who often have sophisticated tools, are well-funded, highly skilled, and focus on conducting both tactical and strategic operations ranging from establishing long-term access footholds in systems or networks to disrupting campaigns (e.g., false flag, fake news, and influence). They employ various techniques, such as exploiting supply chain intermediaries to include injecting exploits into software provided by public open-source repositories, software distributors, and defense industrial base (DIB) system integrators (SIs). Through infiltrating these trusted entities, they can inject malicious code, tamper with software components, or manipulate updates to distribute compromised software [13, 17].

For example, attackers inject malicious code or malware into legitimate software packages during development, distribution, or updates within publicly available repositories where key modules for enterprise software builds are staged. This can result in compromised software being delivered to end-users, allowing attackers to gain unauthorized access or control over systems. Nation-state and APT campaigns seek efficient (cost and time) means of gaining footholds within organizations. Herr [13] suggested that many of the SSC attacks have gone unreported since many of the dependencies or third-party libraries used in software development are exploited through embedding backdoors into the software, potentially leading to unauthorized access or data breaches. This current state encourages providers of software components for SSCs to embrace layered defense-in-depth approaches [18] that employ behavioral-based detections with AI, coupled with both software frameworks [16, 19], blockchains [20], and governance/compliance frameworks [1].

PROPOSING LAYERED SSC SECURITY

Establishing mechanisms to verify the integrity and authenticity of software components throughout the SSC is the goal of any enterprise that depends on software sourced from multiple third-party providers. Gaps in existing approaches to SSC security suggest the need for a comprehensive defense-in-depth strategy that involves layering software frameworks to achieve the following:

- Improve metadata cataloging of software artifacts (e.g., implementing TUF and/or in-toto on artifacts),
- Use AI in behavioral-based detection approaches (i.e., use AI models to identify anomalies and points of compromise within an SSC),
- Implement a private or public blockchain to serve as an immutable

> ***Gaps in existing approaches to SSC security suggest the need for a comprehensive defense-in-depth strategy.***

electronic data structure to enable on- and off-chain comparisons of SSC components, and

- Align with the supply chain Identify portion (ID.SC) of the NIST CSF best practice recommendations [1].

When working in tandem, these layers can suggest major improvement proposals for SSC security wherein integration across each can support comprehensive SSC security. Such integrated measures offer better protection against mix-and-match attacks, malicious mirrors, and key compromise vulnerabilities (e.g., single or threshold of keys). Support of layered SSC security involves implementing best practices of access, validation control, and code change management to preserve the integrity of repository code commits (see Figure 4) [21].

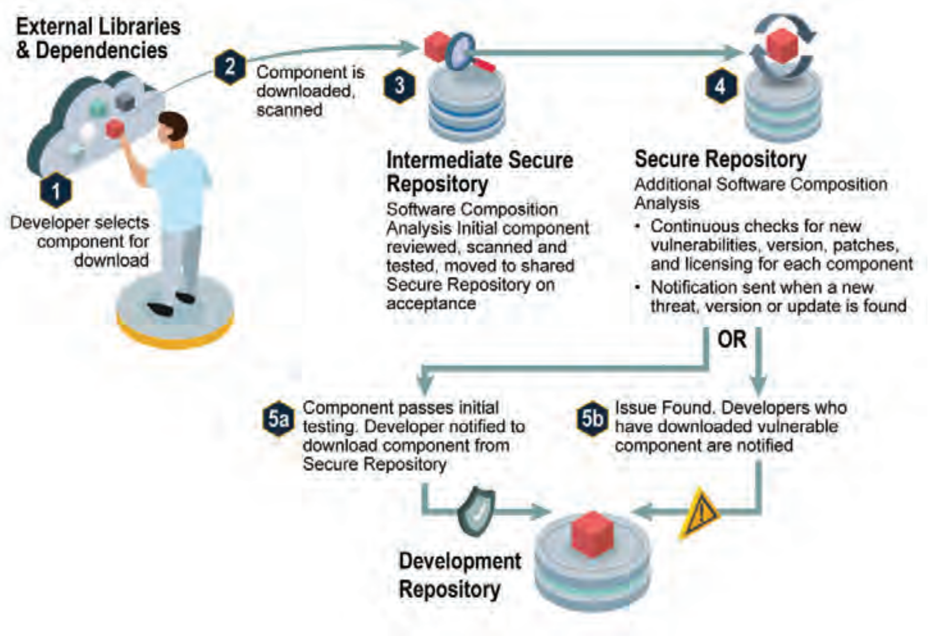

External Libraries & Dependencies
1
Developer selects component for download
2
Component is downloaded, scanned
3
Intermediate Secure Repository
Software Composition Analysis Initial component reviewed, scanned and tested, moved to shared Secure Repository on acceptance
4
Secure Repository
Additional Software Composition Analysis
• Continuous checks for new vulnerabilities, version, patches, and licensing for each component
• Notification sent when a new threat, version or update is found
OR
5a
Component passes initial testing. Developer notified to download component from Secure Repository
5b
Issue Found. Developers who have downloaded vulnerable component are notified
Development Repository

Figure 4. Secure Software Commit Process *(Source: U.S. National Security Agency [NSA], Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI) [21]).*

The in-toto framework (intoto.io) is a system designed to secure the entire SSC, encompassing the development, building, testing, and packaging processes. It provides attestation of integrity and verifiability for each action performed throughout the supply chain, including code writing, compilation, testing, and deployment. The framework ensures transparency by disclosing the order of steps and actors involved. According to in-toto [19], the framework enables users to verify the intended execution of each step, authenticate the actors involved, and ensure that materials (such as source code) remain untampered between steps. TUF empowers developers to safeguard updated systems against repository compromises and attacks that focus on signing keys. It offers a robust approach to provide trust information about software, including meta-information about artifacts. Its primary objective is to authenticate the source of data stored in repositories. Additionally, it verifies the freshness of artifacts and maintains repository consistency, which are crucial steps for ensuring overall integrity and security in SSCs. TUF aims to prevent malicious behavior where attackers manipulate software artifacts in a way that the combined result can become malicious [16].

SSCs rely on Software Bill of Materials (SBOM) manifest data from various sources. Manipulation of this metadata has been shown to be an integral part of an SSC attack [17, 20]. To address this SSC security gap, researchers have suggested integrating a private blockchain to remove the hacker's ability to alter SBOM entries [22]. Blockchain's decentralized and immutable nature provides a transparent and tamper-resistant ledger for SSC security by tracking software components, verifying their integrity, and enhancing supply chain transparency. It provides an immutable and decentralized ledger that enhances trust and accountability in the supply chain [17]. An example has been demonstrated by Let'sTrace, which combines blockchain technology, federated learning, and both TUF [16] and in-toto [19] to enhance provenance in the cyber supply chain. Let'sTrace leverages blockchain technology to enable "smart contracts" for blockchain transactions, which establishes an immutable and transparent ledger for monitoring supply chain activities with greater efficiency and speed.

Two examples exist within the literature that could potentially support blockchain integration for SSCs. First, Let'sTrace incorporates TUF and in-toto frameworks to provide secure software updates and ensure the integrity of each step in the supply chain. As discussed earlier, these frameworks verify the authenticity and integrity of software components, preventing unauthorized modifications and ensuring trustworthiness throughout the supply chain [22]. Second, DeepChain is an intelligent framework for SSC security based on blockchain technology that integrates ML techniques to analyze software artifacts, detect anomalies, and identify potential security risks or vulnerabilities using a consensus mechanism based on the blockchain network to ensure the immutability and transparency of SSC activities [23]. Its enhanced data privacy and secure communications within the supply chain align with governance best practices through enhanced traceability, improved security auditing, and efficient collaboration among supply chain participants.

AI MODELS

AI models present multifaceted utilities for improving SSC security. AI algorithms can analyze vast amounts of data, detect patterns, and identify anomalies, allowing for faster and more accurate security assessments. (Note: A detailed discussion about specific AI approaches is beyond the scope of this article; however, Bandara et al. [22] provide ample motivation and treatment for the subject, leveraging a federated learning approach in support of SSC security.)

For SSCs, AI forms one layer of the proposed defense in-depth strategy to provide risk assessment associated with software components, repositories, software providers, DIB SIs, and other SSC providers within the supply chain. For example, AI that continuously assesses vendor reputation and their security track record (e.g., an analog to the three-digit consumer credit score used by vendors to track and rate financial risk) can be a source of enrichment for making informed decisions for selecting and managing software suppliers and alerting security operators if vendors fall below an accepted threshold [24, 25].

A core goal of AI is to integrate within current workflows and tools to automate and orchestrate various security processes within the SSC. This includes automating vulnerability scanning, threat detection, and incident response for improving response times and enabling efficiency in workflows. These techniques are being employed to establish baseline behaviors and analyze deviations to help identify potential security threats, including malicious code injections, unauthorized access, and unusual patterns of behavior (Microsoft research has active efforts in this area; see Figure 5). AI enables predictive analytics in SSC security. By analyzing historical data, AI models can forecast potential security risks and vulnerabilities, helping organizations proactively address them before they manifest.

Predictive analytics also assist in risk assessment, identifying weak points in the supply chain and implementing

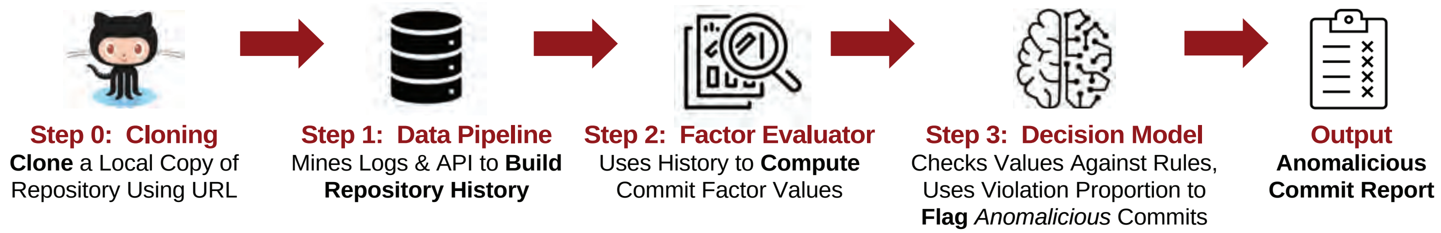

Step 0: Cloning
Clone a Local Copy of Repository Using URL
Step 1: Data Pipeline
Mines Logs & API to Build Repository History
Step 2: Factor Evaluator
Uses History to Compute Commit Factor Values
Step 3: Decision Model
Checks Values Against Rules, Uses Violation Proportion to Flag *Anomalicious* Commits
Output
Anomalicious Commit Report

Figure 5. Overview of the Commit Detector Components, Data Flow, and Output in the "Anomalicious" Tool Proposed in 2021 *(Source: Gonzalez et al. [26]; Made Available by CC BY 4.0).*

preventive measures. AI-powered tools are being used to gather, analyze, and share threat intelligence across the SSC ecosystem. These tools typically consist of the following components: (1) enterprise order management validation through attestations, (2) audit trails for provenance (i.e., artifact creation, lineage, and modification), and (3) audit trail integration for people-product integrated SBOMs (e.g., products like ActiveState, GitLab, and Tenable can support these functions). Disseminating actionable intelligence to relevant stakeholders promotes process efficiencies through collaboration and enables a more comprehensive approach to security across the supply chain. A necessary element of AI consists of identifying potential vulnerabilities in software components/modules/libraries to ensure compliance with security standards while recommending secure coding practices. Development Security Operations (DevSecOps) pipelines can effectively incorporate AI into the build process/development lifecycle to enable organizations minimization of vulnerabilities injected by bad actors that could be exploited in the supply chain [27].

AI-powered systems can continuously monitor an SSC in real-time, detecting suspicious activities and unauthorized access. AI is well-suited for automation of regular security audits and assessments of the SSC to identify potential vulnerabilities, risks, and gaps in security controls (i.e., alignment with RMF, C-SCRM, and CSF). This enables organizations to proactively address potential exploits and vulnerabilities while receiving timely alerts to facilitate more rapid response to security incidents and mitigate potential damage. In addition, the ability to instrument AI in conjunction with security documentation workflows can facilitate autocompletion and updating of required compliance documentation. AI can also be engineered within workflows in security orchestration automation and remediation (SOAR) tools to automate various security processes, reducing manual effort and increasing efficiency. Tasks such as vulnerability scanning, threat intelligence analysis, and incident response can be actively integrated within SOAR and/or DevSecOps pipelines, freeing up security personnel from manually intensive processes to focus on more complex issues [24, 25, 27].

The ID.SC portion of Identify within the NIST CSF [1], the best practices within C-SCRM recommendations [2] and RMF [3] for SSC security, provide high-level guidance to identify, assess, and mitigate risks introduced through supply chain vulnerabilities. These all lend themselves to governance workflows and processes that center around collaboration, communication, and documentation between various parties and stakeholders within an organization.

CONCLUSIONS

The integration of AI in SSC security could empower both military and key national security SSC systems to enhance their threat detection, response capabilities, operational efficiency, risk assessment, and overall resilience against cyberthreats. Effective AI-enabled systems can empower leadership to stay ahead of emerging risks, protect critical systems, and safeguard sensitive information–together significantly enhancing the security posture of the nation. By leveraging AI in a layered, defense-in-depth SSC security architecture, the government can improve its ability to detect and respond to attacks, secure critical systems, and maintain the integrity of the SSC, thereby enhancing overall cybersecurity readiness. ■

REFERENCES

[1] NIST. *Framework for Improving Critical Infrastructure Cybersecurity* (*CSF*). Version 1.1, https://www.nist.gov/cyberframework/framework, 16 April 2018.

[2] NIST. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. Special Publication 800-161 Revision 1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf, May 2022.

[3] NIST. "NIST Risk Management Framework (RMF)." Special Publication 800-5, https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/downloads, 6 July 2023.

[4] Tucker, P. "How DoD Is Experimenting With AI for Enhanced Cybersecurity." *DefenseOne*, https://www.defenseone.com/technology/2023/05/how-dod-experimenting-ai-enhanced-cybersecurity/385922/, 3 May 2023.

[5] Dretzka, E. "Technical Exchange Patterns With [x]BOMs." DoD CDAO, https://repo1.dso.mil/

platform-one/bullhorn-delivery-static-assets/-/raw/master/cso/community-of-practice/04-13-2023-DevSecOps-CoP-SW-Modernization-I-Plan-FINALv3.pdf, pp. 23–34, 14 April 2023.

[6] Red Hat, Inc. "What Is Software Supply Chain Security?" https://www.redhat.com/en/topics/security/what-is-software-supply-chain-security, 14 December 2022.

[7] Zetter, K. "The Untold Story of the Boldest Supply-Chain Hack Ever." *WIRED*, https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/, 2 May 2023.

[8] Wong, W. "Keep Software Supply Chains Secure With New Federal Guidance." *FedTech Magazine*, https://fedtechmagazine.com/article/2023/03/keep-software-supply-chains-secure-new-federal-guidance, 7 March 2023.

[9] U.S. GAO. "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents." GAO-22-104746, report to congressional addressees, https://www.gao.gov/products/gao-22-104746, 13 January 2022.

[10] The White House. *National Cybersecurity Strategy Implementation Plan*. Washington, DC, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf, 13 July 2023.

[11] U.S. DoD. "Supply Chain Risk Management Framework, Project Report – Phase I." OASD(S), https://www.acq.osd.mil/log/LMR/.scrm_report.html/DoD_SCRM_Framework_ Report_Phase_I.pdf, 15 February 2023.

[12] U.S. GAO. "Information and Communications Technology: DoD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks." GAO-23-105612, report to congressional committees, https://www.gao.gov/assets/gao-23-105612.pdf, 18 May 2023.

[13] Herr, T. "Breaking Trust– Shades of Crisis Across an Insecure Software Supply Chain." Presentation at the USENIX Enigma 2021 conference, virtual seminar, https://www.usenix.org/conference/enigma2021/presentation/herr, 2 February 2021.

[14] Boyens, J., C. Paulsen, N. Bartol, K. Winkler, and J. Gimbi. "Key Practices in Cyber Supply Chain Risk Management: Observations From Industry." NIST Interagency Report 8276, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf, February 2021.

[15] Samuel, J., N. Mathewson, J. Cappos, and R. Dingledine. "Survivable Key Compromise in Software Update Systems." New York, NY: Association for Computing Machinery, Proceedings of the 17th ACM Conference on Computer and Communications Security, https://doi.org/10.1145/1866307.1866315, October 2010.

[16] TUF. "Overview." https://theupdateframework.io/overview/, accessed on 20 July 2023.

[17] Shetty, S. "Assured Cyber Supply Chain Provenance Using Permissioned Blockchain." Project overview, University of Illinois Urbana–Champaign, https://iti.illinois.edu/credc/researchactivity/assured-cyber-supply-chain-provenance-using-permissioned-blockchain, 2020.

[18] U.S. Department of Homeland Security. "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies." Industrial Control Systems Cyber Emergency Response Team, https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf, September 2016.

[19] in-toto. "What Is In-Toto?" https://in-toto.io/in-toto/, accessed on 20 July 2023.

[20] Shetty, S. S., C. A. Kamhoua, and L. L. Njila, eds. *Blockchain for Distributed Systems Security*. Hoboken: John Wiley & Sons, 2019.

[21] U.S. NSA, CISA, and ODNI. "Securing the Software Supply Chain: Recommended Practices Guide for Developers." Ensuring Security Framework (ESF) Working Panel, https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF, August 2022.

[22] Bandara, E., S. Shetty, A. Rahman, and R. Mukkamala. "Let'sTrace — Blockchain, Federated Learning and TUF/In-Toto Enabled Cyber Supply Chain Provenance Platform." Presented at the 2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, https://doi.org/10.1109/MILCOM52596.2021.9653024, 29 November–2 December 2021.

[23] Weng, J., J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo. "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive." *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, https://doi.org/10.1109/TDSC.2019.2952332, 1 September–October 2021.

[24] Yang, J., Y. Lee, and A. P. McDonald. "SolarWinds Software Supply Chain Security: Better Protection With Enforced Policies and Technologies." In R. Lee (ed.), *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, Springer, https://doi.org/10.1007/978-3-030-92317-4_4, January 2022.

[25] Singh, S. P., J. Rawat, M. Mittal, and C. Bhatt. "Application of AI in SCM or Supply Chain 4.0." In S. L. Fernandes and T. K. Sharma (eds.), *Artificial Intelligence in Industrial Applications*, Springer, https://doi.org/10.1007/978-3-030-85383-9_4, December 2021.

[26] Gonzalez, D., T. Zimmerman, P. Godefroid, and M. Schaefer. "Anomalicious: Automated Detection of Anomalous and Potentially Malicious Commits on GitHub." Presented at the 2021 International Conference on Software Engineering (ICSE), retrieved from the arXiv database, https://arxiv.org/abs/2103.03846, 9 March 2021.

[27] Akter, M. S., et al. "Software Supply Chain Vulnerabilities Detection in Source Code: Performance Comparison Between Traditional and Quantum Machine Learning Algorithms." The 2022 IEEE International Conference on Big Data, Osaka, pp. 5639–5645, https://doi.org/10.1109/BigData55660.2022.10020813, December 2022.

BIOGRAPHY

DR. ABDUL RAHMAN is a subject matter expert in the design and implementation of cloud analytics and architectures that support situational awareness tools for cyber network operations for commercial and government customers. He has over 25 years of information technology experience, including software development, network engineering, systems design, systems architecture, security, and network management. He has published widely on topics in physics, mathematics, and information technology. Dr. Rahman holds Ph.D.'s in mathematics and physics.

MODELING & SIMULATION

BATTLE READINESS IN A VIRTUAL WORLD

BY BRIAN NIELSON

(PHOTO SOURCE: AUTHOR GENERATED AND CANVA)

INTRODUCTION

As the world becomes more complex, the U.S. Department of Defense (DoD) faces a range of challenges that demands innovative solutions. One tool that has proven invaluable in this regard is modeling and simulation (M&S)—the process of creating a representation of a system or process and then using that representation to explore and test different scenarios. The modeled system can range from a piece of equipment to an entire organization, and the representation can take many forms, including mathematical models, computer simulations, or physical mock-ups (Figure 1).

By using M&S, the DoD can explore scenarios and test concepts without risking personnel or equipment. In this article, we will explore the role of M&S in the DoD, its benefits, and some examples of its use.

Figure 1. Example of a Soldier Using M&S *(Source: Techviz.com [1]).*

> “
>
> ***By using M&S, the DoD can explore scenarios and test concepts without risking personnel or equipment.***

M&S USED BY THE DOD

M&S used by the DoD is created by a range of organizations, including government agencies, defense contractors, and academic institutions [2]. These entities work together to develop M&S that meets the specific needs of the DoD. The DoD has several organizations dedicated to developing and using M&S, including the Defense Modeling and Simulation Coordination Office (DMSCO) and the Defense Advanced Research Projects Agency (DARPA). DMSCO is responsible for coordinating the use of M&S across the DoD, while DARPA focuses on developing advanced technologies that can be used in M&S applications [3].

Defense contractors are important players in developing M&S for the DoD. These companies often have specialized expertise in areas such as software development, systems engineering, and data analytics, all critical for M&S development.

Academic institutions also play an important role in M&S development. Many universities have research programs focused on M&S, and they work closely with the DoD to develop innovative technologies and techniques. The DoD often funds research projects at universities, providing resources and expertise to support M&S development. This involves collaborating between government agencies, defense contractors, and academic institutions, all working together to create effective tools that can support military planning and operations.

The DoD has a joint program to develop an integrated suite of modern computational engineering tools within an architecture that aligns both acquisition and operational business processes (Figure 2) [4]. The suite includes models, simulations, and related capabilities and trade space assessment and visualization tools. The U.S. Army is implementing a lifecycle approach for extensive and complex product data required in the

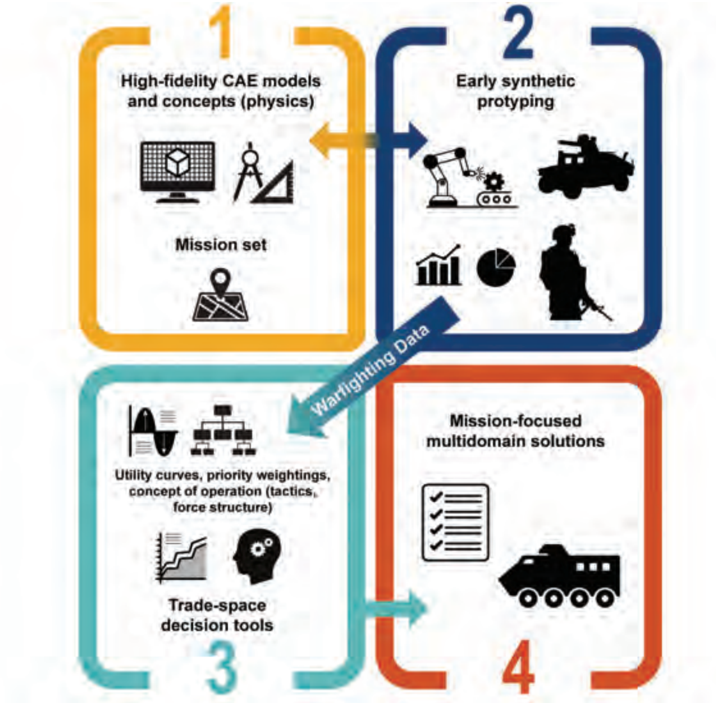

1
High-fidelity CAE models and concepts (physics)
Mission set
2
Early synthetic protyping
Warfighting Data
Utility curves, priority weightings, concept of operation (tactics, force structure)
Trade-space decision tools
3
Mission-focused multidomain solutions
4

Figure 2. DoD Computational Engineering Tools Suite *(Source: U.S. Department of the Army [4]).*

engineering design, acquisition, and sustainment of military systems being adopted by the Army Combat Capabilities Development Command.

THE BENEFITS OF M&S

The benefits of M&S are numerous—the most significant is the ability to explore scenarios and test concepts in a safe, controlled environment. By creating a model of a system or process, analysts can adjust parameters and inputs to see how the system or process reacts. An analyst might model the impact of a particular weapon on a particular target, adjusting variables like range, angle, and projectile type to see how the weapon performs under different conditions. This kind of testing can provide insights that would be difficult or impossible to obtain through live testing. M&S can also be used to explore scenarios that would be too risky, expensive, or time-consuming to test in the real world. For example, an analyst could model the impact of a cyberattack on a military network to see how the network would respond. This kind of testing, also known as chaos engineering (CE), can help identify vulnerabilities and inform the analyst of developing countermeasures.

CE is a discipline that aims to proactively uncover vulnerabilities and weaknesses in complex systems by intentionally injecting failures or disruptions. It involves running controlled experiments in production or testing environments to simulate various real-world failure scenarios and observe how the system responds. The core principle of CE is to expose and address weaknesses before they result in unplanned outages or service disruptions. By intentionally introducing failures, CE helps build resilience, identify potential points of failure, and improve the overall reliability and robustness of systems.

> **“**
>
> ***The benefits of M&S are numerous—the most significant is the ability to explore scenarios and test concepts in a safe, controlled environment.***

It is worth noting that CE should be conducted in a controlled and measured manner, with proper planning and consideration for the potential impact on users and business operations. It is not about inducing chaos indiscriminately but rather using well-defined experiments to gain insights and improve system reliability.

The economic benefits of M&S are just as impressive, including significantly accelerated time to market, drastically increased employment opportunities, whole-market growth, and innovative new products. This is only a glimpse of the potential impacts M&S can have. M&S can offer the following [5]:

- 98% reduction in prototyping and testing
- 25% reduction in safety incidents
- 55% improvement in energy efficiency
- 35% improvement in overall operating efficiency
- 55% reduction in water usage
- 30% reduction in consumer packaging

HISTORY OF M&S AND THE DOD

The DoD has a long history of using M&S. In the 1990s, the Department embraced M&S to explore and test new concepts and technologies. One notable example is the development of the Joint Strike Fighter (JSF) [6]. The JSF program was initiated by the DoD to develop a next-generation, multirole combat aircraft that could replace a variety of existing aircraft across different branches of the U.S. military and be used by international partners.

The JSF program aimed to develop three variants of the aircraft—the conventional takeoff and landing variant for the U.S. Air Force, the carrier-based variant for the U.S. Navy, and the short takeoff and vertical landing variant for the U.S. Marine Corps and the United Kingdom's Royal Navy.

The concept development phase for the JSF program began in 1993, followed by the System Development and Demonstration (SDD) phase in 2001 [6]. The SDD phase involved constructing and testing prototypes to validate the aircraft's design and performance. The first prototype, known as the X-35, made its maiden flight in 2000. The following year, the X-35 was selected over its competitor, the Boeing X-32, to be the basis for JSF production.

Another example in the early 1990s is when The Boeing Company pioneered a new technique of designing a passenger jet entirely using computer M&S (Figure 3) [1]. Compared with traditional design methods used for the Boeing 757 and 767 designs, which involved physical mock-ups, the virtual design process resulted in the following design efficiencies:

- Elimination of >3,000 assembly interfaces
- 90% reduction in engineering change requests (6,000 to 600)
- 50% reduction in cycle time for engineering change request
- 90% reduction in material rework
- 50× improvement in assembly tolerances for fuselage

Engineers utilized M&S to simulate the performance of the aircraft under various scenarios, enabling them to optimize the design and ensure it met the needs of multiple branches of the military and international partners [2].

As time progressed, the DoD expanded the use of M&S to support battlefield planning and decision-making [3]. Analysts also leveraged simulations to model different scenarios, allowing commanders to explore potential outcomes, evaluate strategies, and better prepare for contingencies. To continue future expansion of M&S, the DoD should focus on the following: technology advancements, interoperability, cloud-based solutions, synthetic training environments, scenario diversification, enhanced human-machine teaming, test and evaluation, and adaptive learning.

Figure 3. M&S Used by Boeing *(Source: Techviz.com [1])*.

Recognizing the importance of human performance, the DoD also began utilizing M&S to optimize the capabilities of its personnel. Researchers employed simulations to study factors such as fatigue, stress, and decision-making under pressure. By modeling the impact of these factors, researchers could identify ways to improve training, equipment, and procedures, ultimately enhancing the performance of military personnel [7].

Logistics operations also benefited from the integration of M&S. With the vast scale of DoD operations, analysts used simulations to optimize the movement of personnel, equipment, and supplies. By modeling different scenarios and adjusting variables, such as transportation routes and inventory levels, they identified ways to improve efficiency and reduce costs [8]. In recent years, the increasing reliance on networked systems prompted the DoD to apply M&S to cybersecurity. Analysts simulated cyberattacks and assessed the response of networks, identifying vulnerabilities and developing effective countermeasures to enhance cybersecurity measures [9].

The DoD's use of M&S has evolved into an integral component of defense operations. It has enabled informed decision-making, realistic training, optimized logistics, and strengthened cybersecurity measures. Looking ahead, the DoD will undoubtedly continue to leverage M&S, capitalizing on technological advancements to meet the evolving demands of the defense community [10].

> “
>
> ***In recent years, the increasing reliance on networked systems prompted the DoD to apply M&S to cybersecurity.***

CHALLENGES

While the benefits of M&S are significant, there are also challenges to its effective use. One of the biggest of these is ensuring that models are accurate and represent the modeled system or process. Inaccurate models can lead to flawed insights and recommendations, potentially putting lives and resources at risk. To address this challenge, analysts must ensure that models are based on sound data and validated through testing and evaluation. Another challenge is ensuring that models are accessible and usable by a range of stakeholders. Simulations can be complex and technical, requiring specialized expertise to develop and use. To ensure that models are widely used and contribute to decision-making, they must be developed with the needs and perspectives of end-users in mind.

Finally, there is the challenge of integrating M&S with other decision-making tools and processes. M&S is just one tool in a broader toolkit for decision-making, and it must be used in concert with other tools and processes, such as data analysis and expert judgment. To ensure that M&S is effective, it must be integrated into broader decision-making processes and supported by leadership at all levels.

THE FUTURE OF M&S

The future of M&S in the battlefield holds great potential for further advancements and applications. Increased realism is one of the potential developments that may shape the future of M&S. As computing power and technology continue to advance, M&S simulations will become more sophisticated and realistic. This will allow high-fidelity representations of complex systems, including advanced physics-based models, realistic terrain, and dynamic environments. The result will be more accurate simulations that provide realistic training experiences and improved analysis.

Artificial Intelligence (AI)

Integrating AI is another potential development in M&S. AI technologies can introduce intelligent agents and automated decision-making capabilities within simulations. AI algorithms can generate intelligent adversaries, simulate realistic human behaviors, and support autonomous decision-making, enhancing training, planning, and scenario generation [10].

Augmented Reality/Virtual Reality (AR/VR)

Integrating AR/VR technologies with M&S will offer immersive and interactive training experiences. Virtual environments can replicate real-world scenarios, allowing soldiers to train in realistic combat simulations, conduct mission rehearsals, and familiarize themselves with equipment. Augmented reality can provide real-time information overlays on the battlefield, enhancing situational awareness and decision-making. The advent and increasing use of haptics and touch will enhance immersion in AR/VR M&S applications. Haptics, which involves the sense of touch, plays a crucial role in creating a more realistic and immersive experience for users interacting with virtual environments.

By incorporating haptics feedback, AR/VR developers can add a sense of touch and physical presence to virtual objects and interactions. This technology allows users to feel textures, vibrations, and even the impact of virtual objects, making the experience more engaging and lifelike.

In AR/VR military M&S applications, haptics can have numerous practical benefits, such as the following:

- Training Realism: Haptics can make training simulations feel more authentic, enabling trainees to experience realistic, physical feedback in various scenarios.
- Skill Development: By providing tactile cues, haptics can assist users in developing and refining their skills in a controlled virtual environment.
- Immersive Gaming: In gaming applications, haptics can create a deeper sense of immersion, heightening the overall gaming experience.
- Medical and Healthcare Training: Haptics can be used in medical training simulations to provide students with a more realistic sense of touch when practicing procedures.
- Industrial and Manufacturing Simulation: Haptics can be applied in industrial settings to simulate interactions with machinery and equipment, aiding in training and safety.

The ongoing advancements in haptics technology, such as more sophisticated haptics feedback devices and better integration with AR/VR systems, have contributed to its increased adoption across various industries. As this technology continues to evolve, we can expect even more innovative uses of haptics to further enhance the immersion and effectiveness of AR/VR M&S applications.

Networked simulations will play a vital role in the future of M&S. With the increasing connectivity of military systems, integrating multiple simulations into a larger distributed network will enable collaboration, training, and joint operations virtually. This will facilitate realistic training for multinational forces, testing of interoperability, and evaluation of complex operational scenarios. Advancements in data analytics and machine-learning techniques will continue to benefit M&S.

By analyzing large datasets generated from simulations, analysts can gain valuable insights, identify patterns or trends, and inform decision-making. This supports optimizing strategies and developing new concepts and technologies. Real-time simulation and decision support will be crucial in dynamic situations. Linking simulations to real-time data feeds allows for rapid analysis and decision-making based on the evolving battlefield environment. This integration will provide commanders with the ability to evaluate potential courses of action and predict the outcomes of various tactical and strategic decisions.

Continued interdisciplinary collaboration between military organizations, academia, and industry will be essential for advancing M&S

> ***Real-time simulation and decision support will be crucial in dynamic situations.***

capabilities. Collaboration drives innovation, facilitates the exchange of knowledge and expertise, and fosters the development of innovative technologies. This ensures that M&S remains at the forefront of battlefield training, planning, and decision-making. It is important to note that these developments are speculative and depend on technological advancements, operational requirements, and the evolving nature of warfare. Nonetheless, M&S is expected to continue playing a vital role in training, readiness, and decision support for military forces in the near future [10].

CONCLUSIONS

M&S has become an indispensable tool, transforming the way military operations are conducted. The ability to simulate different scenarios and test concepts in a safe and controlled environment has revolutionized decision-making processes, reduced risks, and enabled the development of innovative technologies and strategies.

M&S plays a significant role in the advancement of defense capabilities, allowing analysts to explore a wide range of scenarios and optimize the performance of military systems.

While challenges exist, such as interoperability of simulation systems, data management, and the validation and verification of models, the benefits of M&S in defense applications are clear—it enables the exploration of new concepts and technologies, enhances training and readiness, optimizes logistics operations, and strengthens cybersecurity measures.

Looking to the future, M&S will continue to play a vital role in defense operations. Technological advancements will drive increased realism, integrating AI and AR/VR and enhancing the immersive and interactive nature of simulations. Networked simulations will facilitate multinational collaboration and interoperability testing, while advanced data analytics will provide valuable insights and support decision-making processes. Real-time simulation and decision support will empower commanders with timely and accurate information, enabling them to respond effectively to dynamic situations. The future of M&S in defense applications is bright, and its ongoing development and utilization will ensure the readiness and effectiveness of our armed forces for years to come [10]. ■

REFERENCES

[1] Techviz.com. "4 Use Cases for Virtual Reality in the Military and Defense Industry." https://blog.techviz.net/4-use-cases-for-virtual-reality-in-the-military-and-defense-industry, accessed on 2 November 2022.

[2] U.S. Government Accountability Office. "Defense Acquisitions: Assessments of Selected Weapon Programs." https://www.gao.gov/assets/320/315527.pdf, March 2011.

[3] DARPA. "Simulation-Based Design." https://www.darpa.mil/work-with-us/simulation-based-design, accessed on 2 November 2022.

[4] U.S. Department of the Army. "Army Modeling and Simulation (M&S)." Army Science Board Fiscal Year 2020 Study, LinkClick.aspx (army.mil), 21 February 2021.

[5] National Training and Simulation Association. "A Primer on Modeling and Simulation." https://www.ntsa.org/-/media/sites/ntsa/homepage/miscellaneous/ms-primer.ashx?la=en, 2011.

[6] JSF Program Office. "The Joint Strike Fighter: A Revolutionary Leap in Technology and Capability." https://www.jsf.mil/downloads/docs/JSF_A_Revolutionary_Leap.pdf, 2003.

[7] Defense Science Board. "Assessment of Directed Energy Technology." https://www.dsc.mil/detechnology, accessed on 24 March 2009.

[8] U.S. Government Accountability Office. "Defense Modeling and Simulation: DoD Needs to Improve Its Management and Guidance to More Fully Leverage Capabilities." https://www.gao.gov/products/GAO-19-64, 20 December 2018.

[9] Defense Logistics Agency. "DLA Energy: Modeling and Simulation." https://www.dla.mil/Energy/Products/Modeling-and-Simulation/, accessed on 2 November 2022.

[10] U.S. Government Accountability Office. "Modeling and Simulation (M&S) in Defense Applications." Defense Industry Information Analysis Center, https://www.dsiac.org/resources/white-paper/modeling-and-simulation-ms-defense-applications, April 2021.

BIOGRAPHY

BRIAN NIELSON is the owner and chief executive officer of Kerns and Bellows Inc. (K+B), a company that specializes in content marketing, brand identity, and market research for defense and commercial companies and military organizations (including classified work) and analyzes data/uses digital media to create marketing and branding campaigns. His proficiency in artificial intelligence and 3-D design has allowed him to create interactive and responsive designs to meet the customers' needs. He began his design and marketing career in broadcast TV in Manhattan, where he crafted visuals and graphics worldwide, and then transitioned into fashion. He also served in the U.S. Marine Corps as an MOS 8541 Scout Sniper, where he earned a triple expert rating for his shooting acumen. Mr. Nielson holds an associate degree from Campbell University and a BFA in graphic design and digital media from New York's School of Visual Arts.

TABLE OF CONTENTS

THE POST-QUANTUM CRYPTOGRAPHY ERA

BY CHADI SALIBY (PHOTO SOURCE: CANVA, GRAPHICSFUEL)

TABLE OF CONTENTS

INTRODUCTION

Safe digital communication for organizations and individuals is protected online by using cryptography, whether making an online purchase from a favorite online store or sending an email to a friend or colleague. Imagine the impact if cybercriminals could break the cryptographic algorithms used to encrypt all our banking, medical information and history, or any sensitive data we use in our day-to-day digital life. As we venture into a time where quantum computing powers could break all conventional encryption methods, the emergence of post-quantum cryptography takes center stage and should be on top of our priorities, providing us with alternatives to keep our digital interactions and data secured. Developing any new quantum-resistant cryptosystems must be done openly and in complete transparency and subjected to rigorous testing and analysis.

A classical computer BIT is a ZERO (0) or a ONE (1), arranged in logical order that makes sense when mapped to a natural language [1]. Quantum computing uses the quantum bit (qubit) as the basic unit of information rather than the conventional bit. Processing information is conducted fundamentally in different ways to the conventional classical computers, which can only be represented by either “1” or “0” of binary information at any single time. Quantum computing uses qubits, which can represent both 0 and 1 simultaneously. This main characteristic of an alternative system of qubits is what permits the coherent superposition of ones and zeros, the digits of the binary system around which all computing revolves [2].

THE QUANTUM THREAT

The previously deemed implausible attacks capable of undermining our current cryptographic algorithms have become feasible due to the emergence of powerful quantum computing, which exploits the principles of quantum mechanics. It is evident that numerous malicious actors and cybercriminals are actively harvesting encrypted data, anticipating that forthcoming technologies will soon break these algorithms—i.e., hack now, crack later [1]. These attacks can result in harvesting and breaking any session key, stealing encrypted and well-protected data from cloud storage. Data encryption is what protects us today in many major breaches, as it renders the data useless in the wrong hands. Conventional cryptographic algorithms like Rivest-Shamir-Adleman (RSA) rely on mathematical large prime equations that are extremely difficult to solve using classical computers. Quantum computing will exploit these inherent patterns and solve those problems exponentially much faster, rendering many existing encryption methods vulnerable to quantum-powered attacks. By making fraudulent digital certificates and deriving private keys from public keys, intercepting any website-encrypted communication becomes an easier task for cybercriminals.

For example, to protect a website and obtain the Hypertext Transfer Protocol Secure (HTTPS) padlock symbol, we use a protocol called Transport Layer Security (TLS) v1.3. The TLS uses a 256-bit key for data encryption and decryption, turning plaintext into ciphertext (Figure 1). In the current computing powers, a supercomputer

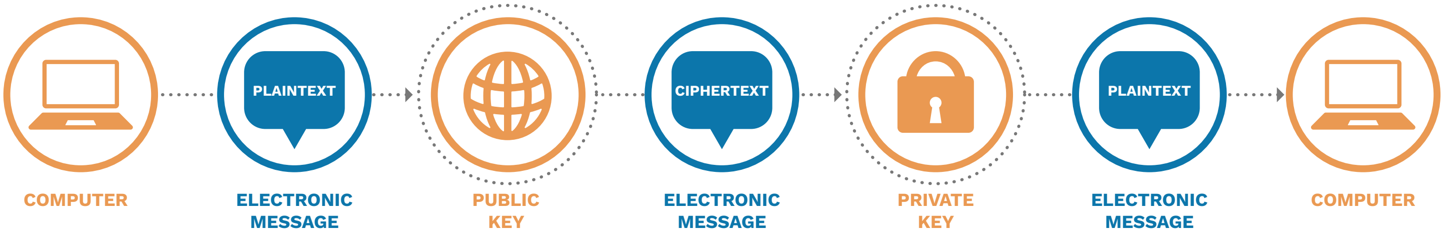


Figure 1. Information Encryption and Decryption *(Source: C. Saliby).*

will take a million years to crack this encryption. Using quantum computing powers to crack the same key will take ~8 hours.

THE QUANTUM CRYPTOGRAPHIC COMPROMISE

In today's encryption, we use symmetric and asymmetric cryptography. Symmetric uses the same key to encrypt and decrypt the data. The most current secure algorithm used is the Advanced Encryption Standard (AES), which can be implemented using 128 bits and 256 bits. The main difference between 128- and 256-bit blocks is that 128 uses 10 rounds of processing to generate keys, while 256 uses 14 rounds of processing to generate keys.

Asymmetric cryptography uses two keys—public and private cryptographic keys in combination. As the name indicates, the public key is given to anyone we want to share the encrypted data with, and the private key is kept well protected in our possession. Mathematically speaking, these keys are very large prime numbers. Examples on asymmetric algorithms are Rivest, Shamir, Adleman (RSA), Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC).

BREAKING BAD IN THE ERA OF QUANTUM

Two important algorithms worth discussing are Shor and Grover. Combining these algorithms with the might of quantum computing powers will easily break most of our current cryptographic algorithms and encryption used today. They were considered and used in analyzing post-quantum cryptography (PQC). Part of the National Institute of Standards and Technology's (NIST's) efforts in initiating a process to solicit, evaluate, and standardize one or more quantum-resistant, public-key cryptographic algorithms, PQC aims to provide a robust security in a quantum-computing landscape, ensuring that encrypted data remains confidential and its integrity is well preserved [3–5].

Several misconceptions surround PQC. One is the notion that achieving quantum-resilient cryptography necessitates the use of quantum computers. Another misconception is the belief that no immediate measures can be taken to safeguard data against quantum-enabled decryption. Similarly, some individuals mistakenly assume that it is solely the responsibility of the Cloud provider to secure their Cloud-based data from quantum threats [1].

Quantum computing, particularly with the Shor algorithm, offers a vastly accelerated approach to solving factoring problems. This includes tackling challenges like integer factorization and elliptic curve and discrete logarithm problem. Consequently, encryption methods such as RSA, DH, and ECC can potentially be compromised within a matter of minutes or hours, as opposed to the previously projected timeframe of thousands of years.

While the Shor algorithm takes care of asymmetric cryptography using factoring, the Grover algorithm will take care of symmetric cryptography by searching for unstructured databases solving function inversion, cutting the brute forcing time of any symmetric algorithm in half. Also known as the Quantum Search algorithm, the Grover algorithm provides a quadratic speedup for unstructured searches using O(√ n) evaluations, speeding searches from (n/2) to (√ n) steps [6].

IS MY ORGANIZATION AT RISK?

The data that requires protection for a prolonged period is the data we must protect (Figure 2). The threat

> **“**
>
> ***Quantum computing offers a vastly accelerated approach to solving factoring problems.***

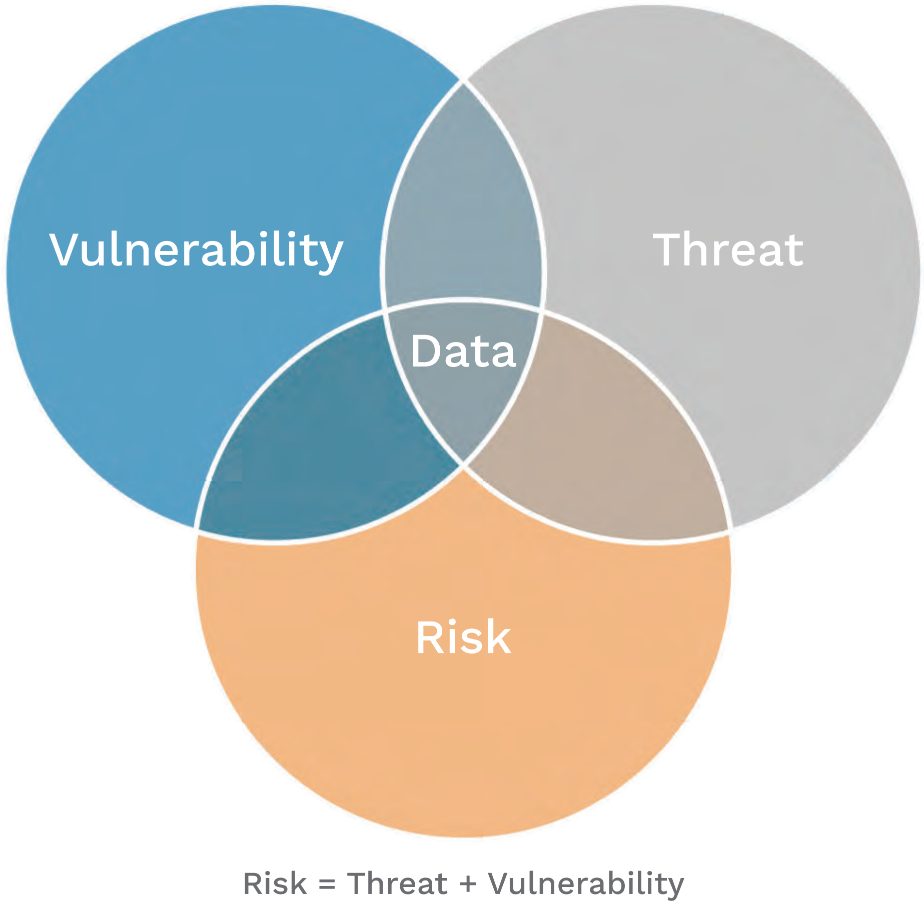


Figure 2. Data at the Core of Any Cyber Risk Assessment *(Source: C. Saliby).*

is now, and the critical impact is soon. Preparing for post-quantum cryptography should be prioritized based on the data's shelf life and system's lifetime durations.

According to a McKinsey study [7], while quantum computers may not be able to crack conventional encryption protocols until 2030, many cybersecurity and risk managers should evaluate their options today.

Using a cryptographically relevant quantum computer will make it very easy to break the traditional algorithmic encryptions currently used. The decision-makers within the cybersecurity industry must start thinking of these problems and act. What was expected to happen in 20 years has started evolving much faster than expected and is taking shape.

ENTERING THE POST-QUANTUM CRYPTOGRAPHY ERA

Many industries and sectors follow rigorous standards, regulations, and industry compliance, one of which is the cryptographic standard dictating what should be used to encrypt sensitive data. An example is using the Federal Information Processing Standard (FIPS) 140-2 with the AES 256-bit keys or the more efficient NIST-approved FIPS 197 or FIPS 180-4, as defined in Special Publication 800-38D for encrypting data at rest [4].

> ***Using a cryptographically relevant quantum computer will make it very easy to break the traditional algorithmic encryptions currently used.***

NIST already announced their six years' competition selection for Quantum-Resistant Cryptographic algorithms [5]:

> "Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

For general encryption and securing website access, NIST selected the Cryptographic Suite for Algebraic

Lattices (CRYSTALS)-Kyber algorithm [8]. Kyber is an IND-CCA2-secure key encapsulation mechanism (KEM) whose security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices. Kyber-512 aims at security equivalent to AES-128, Kyber-768 aims at security equivalent to AES-192, and Kyber-1024 aims at security equivalent to AES-256.

For users interested in using the Kyber algorithm, a hybrid mode combined with an established "pre-quantum" security like the elliptic-curve Diffie-Hellman is recommended. Using the Kyber-768 parameter set will provide decent protection, as it achieves more than 128 bits of security against all known classical and quantum attacks.

Table 1 gives an indication of the performance of Kyber, where the benchmarks were obtained using the Intel Core i7 Haswell central processing unit (CPU). The table displays the key generation cycles (gen), the encapsulation cycles (enc), and the decapsulation cycles (dec). For higher security encryption, NIST selected CRYSTALS-Dilithium, FALCON, and SPHINCS+, recommending CRYSTALS-Dilithium as the primary.

Table 1. Kyber Algorithm Performance [8]

Kyber-512					
Sizes (in bytes)		**Haswell Cycles (ref)**		**Haswell Cycles (avx2)**	
sk:	1632	**gen:**	122684	**gen:**	33856
pk:	800	**enc:**	154524	**enc:**	45200
ct:	768	**dec:**	187960	**dec:**	34572
Kyber-768					
Sizes (in bytes)		**Haswell Cycles (ref)**		**Haswell Cycles (avx2)**	
sk:	2400	**gen:**	199408	**gen:**	52732
pk:	1184	**enc:**	235260	**enc:**	67624
ct:	1088	**dec:**	274900	**dec:**	53156
Kyber-1024					
Sizes (in bytes)		**Haswell Cycles (ref)**		**Haswell Cycles (avx2)**	
sk:	3168	**gen:**	307148	**gen:**	73544
pk:	1568	**enc:**	346648	**enc:**	97324
ct:	1568	**dec:**	396584	**dec:**	79128

The Dilithium algorithm is a digital signature scheme that is strongly secure under chosen message attacks based on the hardness of lattice problems over module lattices. The security notion means that adversaries having access to a signing oracle cannot produce a signature of a message whose signature they have not yet seen nor can they produce a different signature of a message that they have already seen signed [9].

For users interested in using the Dilithium algorithm, a hybrid mode combined with an established "pre-quantum" signature scheme is recommended. Using the Dilithium3 parameter set will achieve more than 128 bits of security against all known classical and quantum attacks.

Table 2 gives an indication of the performance of Dilithium, where the benchmarks were obtained using the Intel Core i7 Skylake CPU. The table displays the key generation cycles (gen), the encapsulation cycles (enc), and the decapsulation cycles (dec).

While we have discussed two of the cryptographic quantum-resistant algorithms announced by NIST, the following other postquantum cryptography protocol proposals are worth mentioning [10, 11].

Table 2. Dilithium Algorithm Performance [9]

Dilithium2					
Sizes (in bytes)		Skylake Cycles (ref)		Skylake Cycles (avx2)	
		gen:	300751	gen:	124031
pk:	1312	sign:	1355434	sign:	333013
sig:	2420	verify:	327362	verify:	118412
Dilithium3					
Sizes (in bytes)		Skylake Cycles (ref)		Skylake Cycles (avx2)	
		gen:	544232	gen:	256403
pk:	1952	sign:	2348703	sign:	529106
sig:	3293	verify:	522267	verify:	179424
Dilithium5					
Sizes (in bytes)		Skylake Cycles (ref)		Skylake Cycles (avx2)	
		gen:	819475	gen:	298050
pk:	2592	sign:	2856803	sign:	642192
sig:	4595	verify:	871609	verify:	279936

- FrodoKEM - A post-quantum cryptography project that is a collaboration between researchers and engineers at Centrum Wiskunde & Informatica (CWI), Google, McMaster University, Microsoft Research, NXP Semiconductors, Stanford University, and the University of Michigan. The International Organization for Standardization has approved FrodoKEM and two other algorithms.
- SIKE and SIDH (Supersingular Isogeny Key Encapsulation) and (Supersingular Isogeny Diffie-Hellman) - Use arithmetic operations of elliptic curves over finite fields to build a key exchange; they are insecure and should not be used.
- Picnic - A public-key digital signature algorithm. Unlike most other public-key cryptographies, Picnic is not based on hard problems from a number theory. Instead, it uses a zero-knowledge proof and symmetric key primitives.
- qTESLA - a post-quantum signature scheme based upon the ring-LWE problem.

CONCLUSIONS

Although post-quantum cryptography holds significant promise, its adoption does not come without major challenges. One main obstacle is transitioning from the conventional established cryptographic methods and algorithms to a new era of algorithms. Organizations must thoroughly and cautiously manage this transition to ensure a flawless shift while maintaining the integrity, availability, and confidentiality of their data.

Failing to plan is planning to fail. From this, the following considerations toward post-quantum cryptography are recommended:

- Create an inventory in which all applications and infrastructure within the environment using public key cryptography are identified.
- Conclude crown jewels data currently protected by public key cryptography.
- Design a clear transition plan for using PQC algorithms within the environment, including testing and adopting new PQC algorithms and retiring the old ones.
- Work closely with all vendors and third parties involved regarding the PQC requirements and maintain clear engagement with all stakeholders regarding the implementation of new algorithms.

One of the projects that users and their organizations should monitor is the Open Quantum Safe project, which is an open-source project that aims to support the development and prototyping of quantum-resistant cryptography. Their liboqs library is a collection designed to further post-quantum cryptography and implementations of quantum-safe KEM and Digital Signature algorithms. They have produced very interesting cryptographic integrations, such as the Post-Quantum Crypto VPN, which is a fork of OpenVPN integrated with post-quantum cryptography; the Post-Quantum Secure Shell (SSH), which is a fork of OpenSSH 7.7; and the Post-Quantum TLS, which is a fork of OpenSSL [12]. ■

REFERENCES

[1] Garris, G. "Quantum Security – Quantum Computing and the Threat to Cybersecurity." Cybersecurity and Information Systems Information Analysis Center webinar, https://csiac.org/webinars/quantum-security-quantum-computing-the-threat-to-cybersecurity/, accessed on 24 August 2023.

[2] Sutor, R. S. Dancing With Qubits: How Quantum Computing Works and How It Can Change the World. Packt Publishing, 28 November 2019.

[3] NIST. "Post-Quantum Cryptography – Security (Evaluation Criteria)." https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria), accessed on 24 August 2023.

[4] NIST. "NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices." https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-smalldevices#:~:text=Currently%2C%20the%20most%20efficient %20NIST,in%20effect%20for%20general%20use, accessed on 24 August 2023.

[5] NIST. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms." https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms, accessed on 24 August 2023.

[6] Quantum Algorithm Zoo. "Algorithm: Quantum Cryptanalysis/Searching/Hidden Shift." https://quantumalgorithmzoo.org/, accessed on 24 August 2023.

[7] McKinsey Digital. "When—and How—to Prepare for Post-Quantum Cryptography." https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/, accessed on 24 August 2023.

[8] Crystals.org. "CRYSTALS – Cryptographic Suite for Algebraic Lattices." Kyber Home, https://pq-crystals.org/kyber/index.shtml, accessed on 24 August 2023.

[9] Crystals.org. "CRYSTALS – Cryptographic Suite for Algebraic Lattices." Dilithium Home, https://pq-crystals.org/dilithium/index.shtml, accessed on 24 August 2023.

[10] Microsoft. "Post-quantum Cryptography." https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/, accessed on 24 August 2023.

[11] Microsoft. "Supersingular Isogeny Key Encapsulation (SIKE)." https://www.microsoft.com/en-us/research/project/sike/, accessed on 24 August 2023.

[12] Open Quantum Safe. "Open Quantum Safe Software for Prototyping Quantum-Resistant Cryptography." https://openquantumsafe.org/, accessed on 24 August 2023.

BIOGRAPHY

CHADI SALIBY is a subject matter expert at CompTIA and Adjunct Professor at Deakin University Centre for Cyber Security Research and Innovation. Prior to his current role, he worked in one of the big four banks in Australia's financial sector as a cybersecurity expert and on the front line of one of the biggest and more successful cybersecurity organizations in their five-star incident response and security operations center team. He acquired various cybersecurity industry certificates from (ISC)2, Microsoft, Cisco, HP, and CompTIA. Mr. Saliby graduated from the Centre International Des Sciences Technique in business computer and programming and continued his MBA Magister en Business et Administration at Sorbonne.

SHARE YOUR
EXPERTISE
If you are a contributing member of the cyber community and are willing to share your expertise, you are a CSIAC subject matter expert.
Register at: bit.ly/46K6Y2g

CSIAC JOURNAL

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a component of the U.S. Department of Defense's (DoD's) Information Analysis Center (IAC) enterprise, serving the defense enterprise of DoD and federal government users and their supporting academia and industry partners.

WWW.CSIAC.ORG
CONNECT WITH US ON SOCIAL MEDIA.