NOV 2021

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

2022-2026 STRATEGIC TECHNOLOGY ROADMAP VERSION 4

SUMMARY

Message FROM THE Chief Technology Officer

CISA Colleagues and Partners,

CISA continues to build on the opportunities to stand up a straightforward, repeatable, and transparent technology investment strategy. Our annual Strategic Technology Roadmap (STR) provides evidence-based recommendations to help you enable and influence future capabilities. I'm hopeful this Summary publication is useful and shows you where we are headed with STR Version 4 (STRv4). Over the next few pages, we'll discuss technology capabilities in development, desired future capabilities, and provide a forecast of the technologies CISA will look to invest in beyond 2026. The STR focuses exclusively on future technology capabilities to address persistent risks imposed by available technologies and future risks discovered from meta-analyses of hundreds of authoritative artifacts, and it is scoped for that purpose.

CISA's mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. Guiding CISA technology investment towards the right mix of technology capabilities to best serve this mission is an evolving challenge. The STR serves as an annual touchstone for this challenge by identifying the technologies receiving current investments and revealing the opportunity areas for future growth.

On an annual basis, the STR examines how CISA defends today and secures tomorrow. To understand how we defend today, the STR:

1. Provides well-researched, evidence-based input to critical decision points that affect future CISA technology capabilities;
2. Identifies capability demands based on rigorous assessment criteria and provides recommendations regarding further use and development of technologies to meet the demands;
3. Describes where capability demands identified in the previous STR are carried forward, where applicable, into this version;
4. Forecasts relevant capabilities based on formal research and development (R&D) pipelines; aligning capability demands with capability forecasts; and
5. Speculates over the horizon technologies that could address specific cyber challenges.

STRv4 reveals to CISA and our partners the technology demand areas where increased investment through 2026 would have the greatest net effect. It does this by comparing current and near-term CISA technology investment with meta-analyses of research produced by CISA and our government and industry partners. STRv4 incorporates improved research and analysis methods to provide more accurate linkages and supportive rationale, from findings to recommendations, to form a guide for CISA technology investments.

STRv4 identifies 18 demand areas, organized into three technology domains – Cybersecurity, Communications, and Critical Enablers. We identify actionable recommendations for each demand area.

Looking to the future—the "securing tomorrow" element of our mission—we wrap up STRv4 with our projections of the risks and capabilities beyond 2026 that CISA may further explore. Though some of the aspects of these capabilities may currently exist in limited or isolated instances, when matured, they have great potential for scalable effect. CISA needs to be ready to embrace their development and capture their value as the technology reaches maturity. We welcome collaboration efforts from our colleagues and partners on these exciting future possibilities.

Brian Gattoni

CISA Chief Technology Officer

TABLE OF CONTENTS

MESSAGE FROM THE CHIEF TECHNOLOGY OFFICER i

INTRODUCTION 1

CYBERSECURITY DOMAIN 2

COMMUNICATIONS DOMAIN 14

CRITICAL ENABLERS 21

CAPABILITY FORECASTS: MAPPING 26

TECHNOLOGY SPECULATION: MULTI-DOMAIN 29

DEFINITIONS 31

INTRODUCTION

The Cybersecurity and Infrastructure Security Agency (CISA) Strategic Technology Roadmap's (STR) goal is to maintain and evolve technological superiority over our Nation's adversaries, to protect and defend against critical infrastructure (CI) risks, and to ensure the availability of emergency communications. The STR, which does not describe any particular CISA project and should not be seen as any kind of request for proposals or applications, is designed to guide CISA technology investments with a foundation based on rigorous research and identification of best practices for industry and government cybersecurity and communications capabilities to achieve the agency's mission needs. Degradation, destruction, or malfunction of government and CI systems could cause devastating human and economic harm to the American people and ultimately pose a threat to the national security of the United States (U.S.).

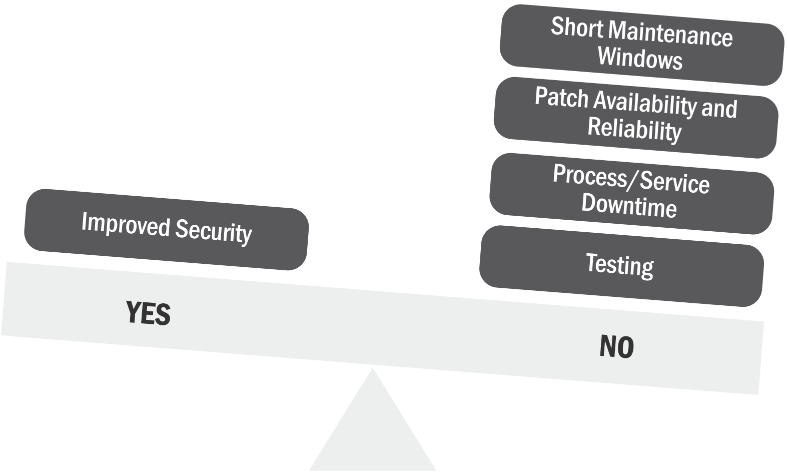
To address these threats and enable CISA's mission, the CISA Office of the Chief Technology Officer (OCTO) develops the STR through a continuous cycle of technology analysis, risk prioritization, future capability definition, and strategy integration, guiding the CISA technology investment within a complex set of competing technology priorities. The STR process reviews previous recommendations annually to account for technology trends, breakthroughs, and commercialization, as well as changing CISA priorities and capability demands. This annual update ensures the STR is responsive to the development and deployment of new CISA capabilities and to the evolution of adversary techniques.

The STR supports and integrates with CISA strategic planning documents and it bridges tactical and strategic planning by providing a framework and context from which to make well-informed investment decisions that ensure CISA is interoperable, efficient, and responsive to national security priorities and, more specifically, the agency's mission. The STR provides succinct findings and recommendations from a broad and deep forward-looking view; it facilitates the execution of the agency's strategies by describing technologies that will enable the CISA mission. Continuous alignment between the STR and CISA strategy will ensure capability demands and capability forecasting not only reflect the results of, and response to, findings reported in security and vulnerability assessments; but also define the capabilities and technologies necessary for the evolution of CISA and its support and services to Federal, State, Local, Tribal, and Territorial (FSLTT) governments, as well as CI owners and operators. Furthermore, creating a STR view into capability demand and capability forecasting enhances decision-making, prioritization, budgeting, and programming for processes, offering a more predictable, integrated, and intentional technology acquisition process and timeframe.

This summary report presents findings and recommendations in the form of "slick sheets", single page summarizations of technologies categorized as capability demands, capability forecasts, and technology speculation. Each slick sheet is intended to address important questions such as: (1) what the technology is; (2) what are the STR's findings or recommendations; (3) why this technology is significant to CISA; and (4) is the described technology something CISA should operate or apply to consultations with FSLTT, private industry, and other partners.

ICS SECURITY

ICS Patching



Industrial control systems (ICS) often fail to receive software patches in a timely manner. ICS owners and operators fail to apply patches for many reasons, including the risk or cost of disruption of operational processes and the failure of vendors to provide patches for specific equipment. Regardless of the reasons, the failure to apply patches leaves ICS devices and systems vulnerable for much of the time they operate. Left unaddressed, the vulnerabilities can threaten production or safety. The potential impacts of not patching include physical destruction of equipment or facilities, economic losses, and personal safety incidents.

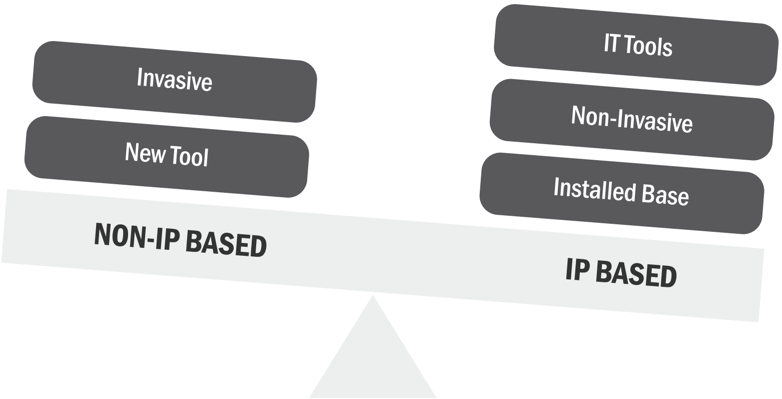
Patch management technology and processes can reduce ICS vulnerabilities. Patch management processes include analyzing patches for criticality, time sensitivity, and testing requirements, which can improve patch deployment decisions and timelines. Additionally, automation of patch deployment could assist in expediting the patching process. Automation can include unit and system testing, as well as patch deployment.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
ICS Patch Management	ADOPT				
ICS Patch Automation	R&D				

Given the potential for cascading failures from attacks on ICS systems in the CI sectors, CISA should consider supporting R&D efforts to improve ICS Patching Automation. Organizations such as Electric Power Research Institute (EPRI) and Pacific Northwest National Laboratory (PNNL), among others, are working to improve the cybersecurity of ICS environments (networks and devices). CISA should also support efforts to encourage CI operators to adopt ICS patch management capabilities. These efforts can reduce the probability of successful cyber-attacks on private and Federal, State, Local, Tribal, and Territorial (FSLTT) operated CI.

ICS SECURITY

Non-IP Based SCADA/ICS Protocol Monitoring



Non-IP based Supervisory Control and Data Acquisition (SCADA)/Industrial Control System (ICS) communications encompass the serial communications between ICS devices, e.g., programmable logic controllers (PLCs) and remote terminal units (RTUs), and the system controller/server containing the human machine interface or graphical user interface. These communications protocols were designed for the exchange of control messages and sensor data, incorporating simplicity, efficiency, and scalability, with minimal security features, such as mutual authentication and encryption. The primary ICS management and control protocols are Modbus and Distributed Network and Protocol 3 (DNP3).

Several capabilities can be combined to address this capability demand, including network monitoring, ICS protocol intrusion detection system (IDS), ICS protocol intrusion prevention system (IPS), and process monitoring systems. Serial interface/network monitoring devices allow for ICS protocols communicated via serial interfaces to be monitored and enables detection of anomalous activity at the serial interface of an RTU or PLC. ICS protocol IDS is a capability that can alert on the detection of anomalous packets. ICS protocol IPS is a capability that can block and alert on the detection of anomalous packets. ICS process monitoring is a capability that monitors the ICS process data collection and control activity to “learn” the “typical” combination of sensor data and commands used to control one or more processes. Process monitoring can be implemented independent of other security capabilities.

Until recently there were no products available that provided adequate monitoring of these protocols. However, new technology is being commercialized into products that address this capability demand.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Serial Interface Protocol (network) Monitoring	ADOPT				
ICS IDS/IPS	ADOPT				
ICS Process Monitoring	ADOPT				

Although ICS operators across multiple sectors rely on the same protocols, their processes are often unique to their environment. Thus, the exploitation of a given operational technology vulnerability may have different impacts depending on the environment. Further efforts should consider how to conduct proof-of-concept vulnerability exploitation tests, identify similarities across sectors, and seek ways to translate vulnerability information into actionable threat intelligence that ICS monitoring solutions can consume in an automated fashion. CISA should adopt this technology, consider how to adapt it to specific critical infrastructure (CI) sectors to illustrate its value to the ICS operators of the nation, and encourage adoption by CI.

ICS SECURITY

Fault Tolerant/Resilient Cyber Physical System

Supervisory Control and Data Acquisition (SCADA) and industrial control system (ICS) systems control processes that combine, modify, and transfer inputs to create outputs by manipulating physical devices or objects. A few examples of controlled processes with large moving parts (e.g., turbines, motors) are energy generation, manufacturing, and ship control. In these, and similar, use cases, the inertia of the devices or objects under control can protect the systems. Inertia is a physical property of matter described as the resistance of a physical object to a change of its speed or direction when an external force acts on that object. ICS can utilize the inertia of the physical components within the process under control to detect and mitigate attacks on the process. An example is the inertia of a rotating steam turbine in an electricity generation plant. The inertia of the turbine can be exploited to protect the process under control (electricity generation), when coupled with security components that detect and mitigate anomalous ICS commands in near real time.

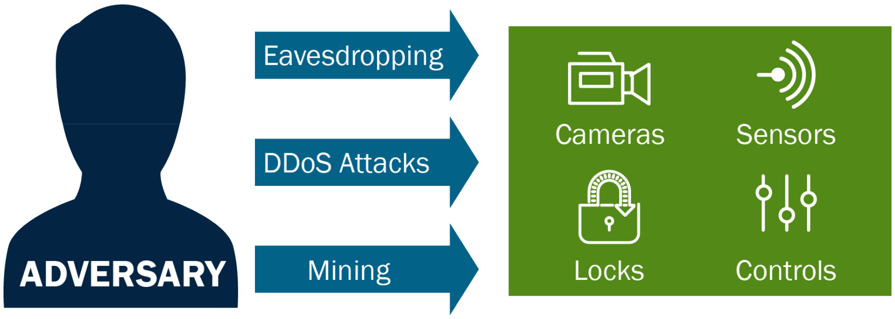
A current research project within the Office of Naval Research (ONR) has developed an ICS control technology using this principle, termed Resilient Hull, Mechanical, and Electrical Security (RHIMES). The candidate technology uses a fault tolerant/resilient cyber physical system (CPS) approach to ICS monitoring and anomalous activity mitigation. The technology includes redundant ICS devices at each process control point, ICS device monitoring, physical system interface switching, local process control point, and automated mitigation control.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Fault Tolerant ICS/ RHIMES Technology	DEMO				

CISA should support further demonstrations of this technology. The goal is to communicate to CI sectors that this technology is valuable. The benefit is a reduced risk probability of successful cyber-attacks on operational technology (OT) systems.

Images Sources: Turbine Image - Time. (2015). The Renewable Energy Source That's About to Boom Again. Retrieved from https://time.com/3978215/hydropower-us-growth/ Digital Lock Image - DOE. (2021). Cybersecurity. Retrieved from https://www.energy.gov/national-security-safety/cybersecurity

IoT SECURITY



Billions of small devices that have a sensor, a network connection, and are designed to run stand-alone, otherwise known as Internet of Thing (IoT) devices, are being used in a very diverse set of applications. More recently, the use of IoT devices has grown within the CISA mission space to perform critical remote sensing, industrial control, and physical security tasks.

Unfortunately, IoT devices usually lack traditional end point security features and other controls. As a result, threat actors use them to eavesdrop to obtain sensitive information, compromise control of the devices or the systems to which they are attached, or to repurpose IoT devices by installing malware to conduct large scale denial of service attacks or cryptocurrency mining operations.

Because of the growing use and criticality of IoT devices and networks, both government and industry continue to develop better security controls for these devices. These technologies include network and on-board botnet detection, and vendor specific and NIST-proposed on-boarding protocol standards. Better on-boarding protocols help to prevent attackers from compromising IoT devices; and botnet detection identifies if a device is controlled by an adversary, so that the device can be disabled or isolated.

In-network botnet detection and vendor specific onboarding protocols are available now, while on-board botnet detection and NIST-proposed standardized on-boarding are still in development.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Botnet Detection (on-board)	R&D				
Botnet Detection (in-network)	ADOPT				
On-boarding Protocols (NIST proposed)	R&D				
On-boarding Protocols (vendor specific)	ADOPT				

CISA should continue to track R&D efforts by NIST and industry to develop botnet detection and NIST-proposed protocols until the availability improves. CISA should adopt internally and encourage critical infrastructure (CI) and Federal, State, Local, Tribal, and Territorial (FSLTT) stakeholders to immediately adopt in-network IDS specifically configured to monitor malicious botnet behavior in IoT devices. CISA should adopt internally and encourage CI and FLSTT stakeholders to replace old IoT devices with new devices that incorporate the latest versions of security features offered by IoT consortiums.

LARGE SCALE ANALYTICS

Image Processing and Deepfake Detection

Image processing can be defined as the technical analysis of an image using complex algorithms. Image processing is also commonly referred to as computer vision. However, computer vision is more narrowly defined as the ability for machines to perceive and act on data in images and video to perform visual tasks (e.g., navigating an environment, labeling a photo). Computer vision is a subdomain of artificial intelligence (AI) whose goal is to give machines a high-level understanding of visual imagery in a way that approaches or simulates human understanding.

Using machine learning (ML), computers can realistically synthesize a person's voice using only seconds of their speech, as well as create images and video depicting fake situations that look real. These technologies are rapidly improving, much faster than research on developing technologies to detect fake speech, video, and images. These concerns draw attention to the disinformation risks that ML poses.

Advanced ML technology spans a wide range of algorithms and methods, which can be applied to a diverse set of decision problems. Recent advances in Deep Neural Networks offer ways of training a machine to learn how to classify input data, driven mostly by large quantities of examples.

Deepfake Detection is a special case of image processing that uses multiple factors, such as ML, knowledge of training data sets, digital signatures, and reverse engineering to determine unique patterns within images.

Image processing can be employed to support a wide range of mission activities for CISA and its partners including intelligence and surveillance, visual monitoring of sensitive areas, hazard detection at incident scenes, threat identification, detection of mis/disinformation campaigns, and other risk management and analytic purposes.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Image Processing	ADOPT				
Deepfake Detection	DEMO				

CISA should adopt internally and encourage critical infrastructure (CI) and Federal, State, Local, Tribal, and Territorial (FLSTT) stakeholders to immediately develop and adopt an image processing architecture that provides AI-enabled edge processing and automation to ensure that appropriate analytics and situational awareness are being identified from all captured imagery. CISA should demonstrate deepfake detection internally to further develop techniques, systems, and best practices to enable deepfake detection in acquired images.

Image Source: Zakharov, E., Shysheya, A., Burkov, E., & Lemptisky, V. (2019, May 26). Deepfakes Generated from a Single Image. The Technique Sparked Concerns That High-Quality Fakes Are Coming for the Masses. But Don't Get Too Worried, Yet. Retrieved from https://www.wired.com/story/deepfakes-getting-better-theyre-easy-spot/?utm_source=WIR_REG_GATE.

LARGE SCALE ANALYTICS

Homomorphic Encryption

CISA and its stakeholders are faced with the common problem of securely storing, and interacting with, large amounts of data. To mitigate the risks inherent in storing and computing sensitive data (such as misuse, theft, or sabotage), systems employ encryption. Traditional encryption systems, such as those typically used in commercial cloud systems, lock data in a manner which makes it impossible to use or execute computations, while the data is in encrypted form. Homomorphic encryption (HE) is an advance in cryptography that protects data confidentiality. HE enables useful computation on the encrypted data producing the results of the computation in encrypted form, without decrypting the data or requiring access to the decryption key.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
HE	DEMO				

CISA should follow and work closely with the National Institute of Standards and Technology's Computer Security Resource Center project to follow the progress of emerging technologies in the area of privacy enhancing cryptography. CISA should seek opportunities to integrate HE demonstrations into data sharing efforts to preserve privacy while expanding the opportunities to leverage a broader community of research and analytics in cybersecurity defense and cyber threat intelligence.

Image Source: What Is Homomorphic Encryption? And Why Is It So Transformative? ADOBE stock. (2019, November 15). Retrieved from https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/?sh=205b56437e93

LARGE SCALE ANALYTICS

Machine Learning for Analytics

Machine Learning (ML) analytics, with varying degrees of capability, are becoming common across industries and critical infrastructure (CI) sectors. Applications include shopping recommendations, voice recognition, fraud detection, text processing, video/image analysis, process optimization, and facial recognition. Cybersecurity, which has large volumes of available data coupled with a shortage of highly skilled analysts able to make sense of the data, appears well positioned to use ML techniques. Cybersecurity data can come from many sources, such as sensors, systems, networks, cyber threat intelligence feeds, cybersecurity tools, and user behavior analytics. The exponential growth in available cybersecurity data has resulted in the use of two phrases being widely employed: “big data” and “analyst burnout.” Big data refers to the very large sets of data that organizations are accumulating. In some cases, the data sets are well beyond petabyte scale, so large that they require planning to determine how to store, compute, and transport. Analyst burnout acknowledges that human analysts are not able to process or keep up with volumes of data at these scales resulting in a sustainability at scale challenge.

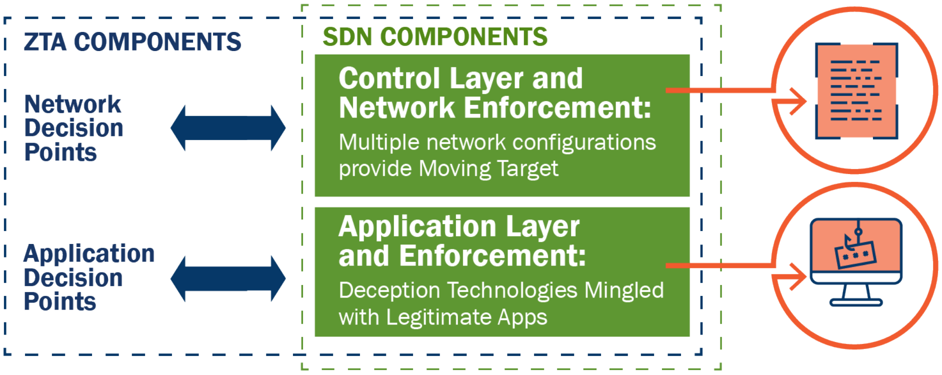
ML can augment both present analytics and analysts, thereby reducing the gap between “too much” data and “too little” skill or staffing levels. ML can detect suspicious (anomalous) events by learning what constitutes normal event behavior, comparing new events to the learned behavior, adapting accordingly to the new behavior, and generating alerts as appropriate. It can also potentially be used to analyze logs for threat hunting.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
ML and Large-Scale Analytics	ADOPT				

CISA should adopt ML integrations into security operations internally and encourage Federal, State, Local, Tribal, and Territorial (FSLTT) and CI stakeholders to implement, as appropriate to their operations centers.

Image Source: PSPN. (n.d.). Vector Brain and Circuit Board, Artificial Intelligence or AI Concept [Royalty-free stock vector ID: 748227748]. Retrieved from https://www.shutterstock.com/image-vector/vector-brain-circuit-board-artificial-intelligence-748227748..

NETWORK SYSTEMS SECURITY



ZTA COMPONENTS

Network Decision Points

Application Decision Points

SDN COMPONENTS

Control Layer and Network Enforcement: Multiple network configurations provide Moving Target

Application Layer and Enforcement: Deception Technologies Mingled with Legitimate Apps

Network security is an organization's strategy and provisions for ensuring the confidentiality, integrity, and availability of the data that is stored, processed, transmitted, or received by computing and communication assets. The objective of network security is to provide security in-depth to the enterprise through a combination of policy, technical enforcement, and security information and event monitoring.

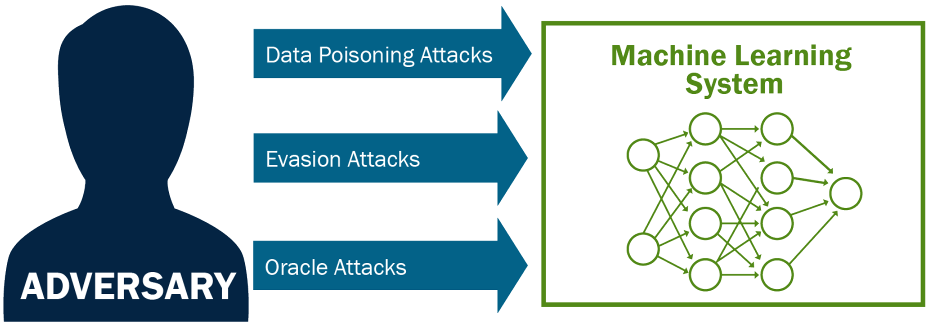
Since even the most robust defenses eventually fail in the face of a determined adversary equipped with sufficient talent, determination, and resources, defenders must recognize that historical cybersecurity approaches based on blocking all intrusions at a network perimeter are insufficient. The concept of cyber resiliency evolved to meet this challenge. Resilient systems can withstand and recover from failures in a way that minimizes both damage to the defender and benefit to the attacker. There are four significant technologies for resilient networks: Deception Technologies, Moving Target Defenses (MTD), Software Defined Networking (SDN), and Zero Trust Architecture (ZTA).

Deception tactics help determine the presence of adversaries on systems, hamper their ability to accomplish their goals, and help defenders identify attackers and their tactics. MTD seeks to introduce randomness, heterogeneity, and dynamism into systems in a way that degrades the advantages enjoyed by attackers in more static environments. SDN enables dynamic, programmatically efficient network configuration, improving network performance and monitoring, and permitting a rapid response to intrusions. ZTA adopts a key premise of resilience – intruders are already on the network – and calls for strict network segmentation and constant reevaluation/enforcement of access rights.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Existing Deception Technology	ADOPT				
Advanced Deception Technology	ADOPT				
MTD	ADOPT				
SDN	ADOPT				
ZTA	R&D				

CISA should adopt SDN, MTD, and Deception Technologies for internal infrastructure and influence Federal, State, Local, Tribal, and Territorial (FSLTT) and critical infrastructure (CI) stakeholders to deploy it. CISA should continue participation in NIST ZTA projects to contribute expertise and to maintain awareness of the NIST guidance changes and lessons learned from proof-of-concepts. Executive Order 14208 has been issued to move towards a ZTA , so steps toward precursor activities should be included in current plans with concurrence of CISA leadership.

RESILIENT MACHINE LEARNING SYSTEMS



Machine learning (ML) systems are designed to emulate the way a human learns. They use data and algorithms to iteratively improve the ability to make classifications, recommendations, or predictions. They can be more effective or efficient than humans in digesting large amounts of data, and quickly and accurately detecting patterns. Because of their ability to classify and predict, ML systems are increasingly being used in the cybersecurity domain and for critical infrastructure (CI) application for many use cases such as malware scanning, intrusion detection, facial and fingerprint recognition, Security Orchestration, Automation and Response (SOAR), and large-scale analytics.

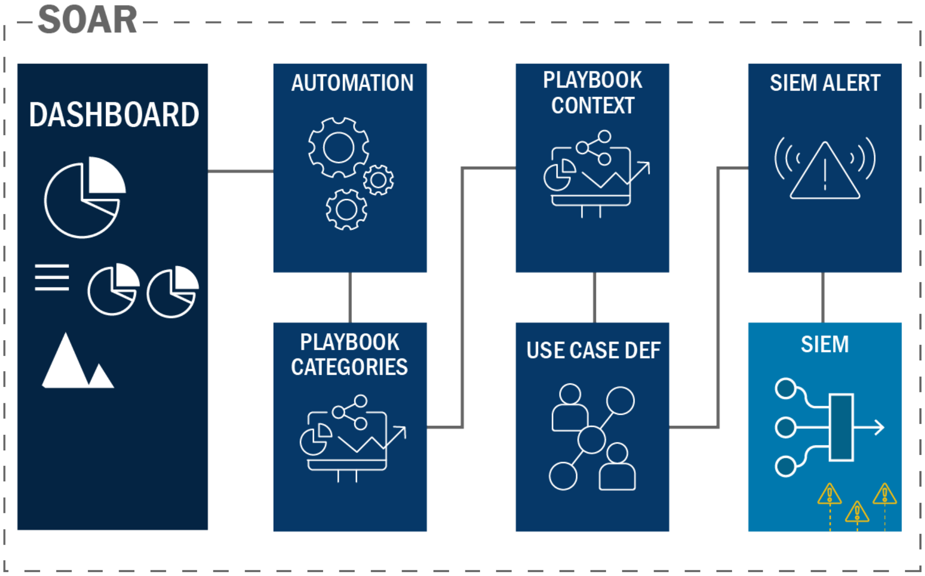
ML systems are vulnerable to attacks that exploit the design, training, and operation of these systems. These attacks can be grouped into data poisoning attacks, where data used to train the system is tainted with bad data to make the model perform differently than expected; evasion attacks, where input data is modified so that the model incorrectly classifies it; and oracle attacks, where an adversary extracts data from the model using successive queries.

Because of the growing use and criticality of ML systems, researchers are developing techniques to prevent these forms of attack. These techniques can be grouped into data poisoning attack defenses and evasion and oracle attack defenses. In general, poisoning attacks are mitigated by detecting or preventing the injection of bad data into the ML training data set, and evasion and oracle attacks can be defended by obscuring training data or making the models less sensitive to perturbations an adversary may use to fool or extract data from the model in operation.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Evasion and Oracle Attack Defenses	MONITOR	MONITOR	DEMO		
Data Poisoning Attack Defenses	MONITOR	MONITOR	DEMO		

Resilient ML techniques are still in development so it is recommended that CISA monitor them until the techniques become more available, which could take several years.

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) EFFECTIVENESS



Security Orchestration, Automation, and Response (SOAR) technologies automate security actions using connections to security sensors and other technology platforms in (or connected to) an organization. SOAR technologies can be configured to execute playbooks or workflows that consist of a series of actions, including response actions (e.g., triage a list of alerts, quarantine a user session, run a vulnerability scan, open a ticket, update a signature, alert an analyst). In this manner, playbooks provide security organizations with a mechanism to automate processes (or portions of processes) that were previously manually conducted by security operations staff.

The SOAR marketplace, through significant vendor investment (in both technology development and acquisitions), is rapidly maturing. Analytics from some vendors now include machine learning (ML) capabilities. SOAR ML capabilities available today come in primarily two forms: 1) the ability to dynamically prioritize items (e.g., alerts generated by other security tools) and 2) the ability to provide recommendations to the security professional (e.g., recommendation to examine a certain endpoint).

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
ML and SOAR	DEMO				

The initial recommendation is to work with selected stakeholder organizations to demonstrate this capability. SOAR solutions are operational at some stakeholder organizations already, and these organizations may be able to provide lessons learned for increased adoption as well as the implementation of advanced SOAR playbooks that leverage ML. This capability has the potential to greatly assist analysts and responders.

The ML component of SOAR tools is in its infancy but will mature over a multi-year period. It is important for organizations that are mature to adopt SOAR now to be in position to take advantage of the incremental advances that are coming. Strategies to avoid vendor lock should be explored as part of this adoption, and CISA should strive to build expertise in SOAR playbooks and requirements for operationalization.

Image Source: OCTO. (2021). Draft CISA Target Architecture

SOFTWARE ASSURANCE AND VULNERABILITY MANAGEMENT

```
clickHandler = fun
href
$this = $(this)
$target = $($this.attr('data-target')
href.replace(/.*(?=#[^\s]+$)/, '')) // st
($target.hasClass('carousel')) return
options = $.extend({}, $target.data(), $
slideIndex = $this.attr('data-slide-to')
(slideIndex) options.interval = false
Plugin.call($target, options)
(slideIndex) {
$target.data('bs.carousel
```

Software assurance is defined as the confidence that software functions as intended and is free of vulnerabilities throughout its lifecycle, irrespective of whether the vulnerabilities are a result of intentional or unintentional actions. In addition to traditional applications, software assurance is important for AI adoption to ensure that expected behavior is maintained as algorithms are retuned.

As application development architectures evolve in DevOps, test automation needs to evolve as well. The application of machine learning (ML) in software testing tools is focused on optimizing the software development lifecycle. The value of applying ML to software testing is achieved by creating opportunities for development teams to focus on software enhancements or other impactful quality assurance activities.

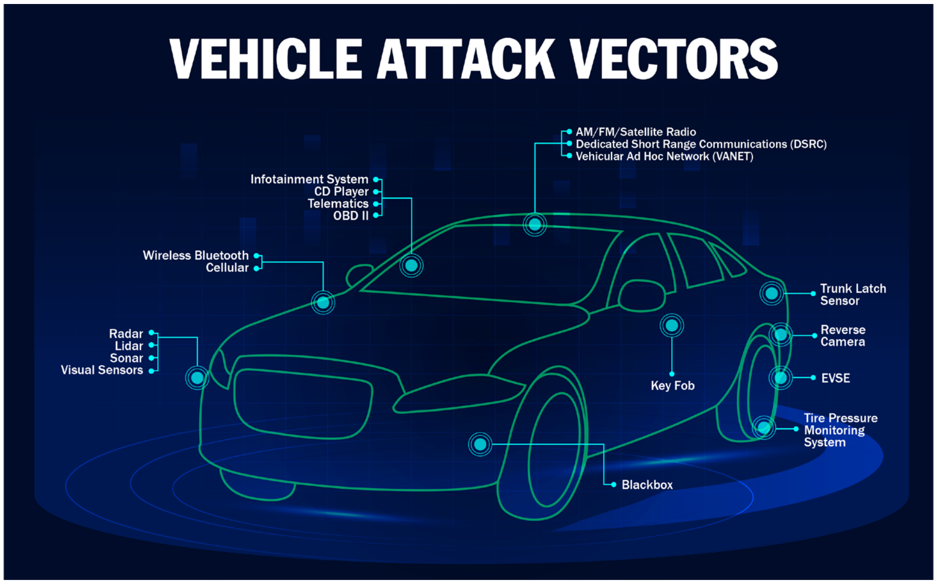
Modern software is complex. In addition to increasing software complexity, there are often many blocks of code within complex systems of software (including the layers of libraries) that are redundant or perform similar functions. Many blocks perform extraneous, seldom-used, or never-used functionality. Feature creep, device-specific optimizations, and attempts to support multiple different architectures all contribute to software bloat. Current software development practices and frameworks encourage this situation (e.g., Object-oriented programming, libraries, deprecated code, layers of abstraction). It is highly desirable to have an enhanced software architecture and deployment strategy that improves software efficiency while preserving the productivity benefits of state-of-the-art development practices. Improving software efficiency by simplifying the structure/layering of the final executable late in the software development lifecycle, while maintaining the benefit of software reuse and layering at the development stage, is an important goal to be addressed in providing secure software.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
ML For Software Testing and Analytics	ADOPT				
Late Life Cycle Binary Reduction	DEMO				

CISA should adopt ML capabilities for software testing internally and encourage Federal, State, Local, Tribal, and Territorial (FSLTT) and critical infrastructure (CI) stakeholders to implement, as appropriate through best practices. CISA should pursue demonstrations internally for late life cycle binary reduction to determine its utility and risk to operations.

Image Source: Jivacore. (n.d.). Software Source Code [Royalty-free stock photo ID: 634574354]. https://www.shutterstock.com/image-photo/software-source-code-programming-on-computer-634574354.

VEHICLE SECURITY



Current automobiles include over 100 million lines of code and 50 to 80 electronic control units, similar to the level of a fighter jet. During the 1970s, manufacturers started using electronics to control engine functions and diagnose engine problems. Through the years, vehicle electronic systems have become more sophisticated. These systems provide almost complete engine control and monitor parts of the chassis, body, and accessory devices, as well as provide functions such as navigation guidance, adaptive cruise control, cellular communication, and interfaces with wireless devices. A consequence of introducing software and electronics is that automobiles are now susceptible to threats similar to those for software development, network infrastructure, Internet of Things (IoT), and Industrial Control Systems (ICS). Vehicle systems also contend with additional attack vectors such as wireless links (e.g., 5G cellular) for over-the-air updates or vehicle-to-vehicle communications.

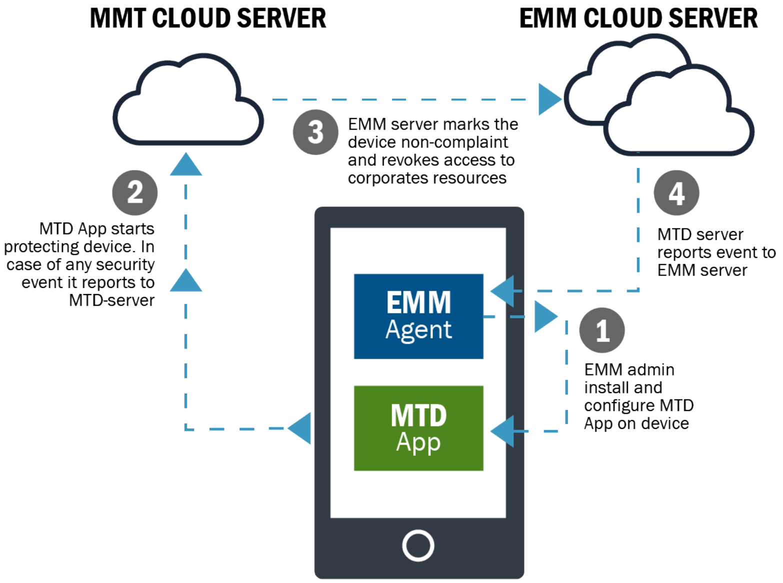
TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Open Architecture Software	ADOPT				
Patching (over the air or via physical link)	ADOPT				
Technical Security Standards and Protocols	ADOPT				

CISA should invest in efforts to continuously improve information sharing, threat intelligence, and existing standards. CISA should encourage CI to recognize and adopt vehicle security technologies as a part of information technology space along with IoT, ICS, and software and hardware development.

Image Source: Department of Energy. (2019). National Renewable Energy Laboratory publication: Vehicle Cybersecurity Threats and Mitigation Approaches.

CELLULAR SECURITY

Enterprise Mobility Mgt, Mobile Threat Defense, Mobile App Vetting, and Network Monitoring


MMT CLOUD SERVER
EMM CLOUD SERVER
3
EMM server marks the device non-complaint and revokes access to corporates resources
2
MTD App starts protecting device. In case of any security event it reports to MTD-server
4
MTD server reports event to EMM server
EMM Agent
MTD App
1
EMM admin install and configure MTD App on device

Cybersecurity technologies that work collectively to improve cellular security include Enterprise Mobility Management (EMM), Mobile Threat Defense (MTD), Mobile Application Vetting (MAV), and Network Monitoring. EMM provides protection at the device level but does not have an ultimate view into the behavior of the applications that execute on the device, whereas MTD monitors these applications. EMM contains the Mobile Device Management (MDM) profile on the device which allows administrators to take actions such as remotely wipe data or the entire device. An EMM agent has to install and configure MTD on devices. After MTD configuration, potential malicious events are noticed by MTD and reported to an MTD server, which in turn, will report the event to the EMM server. The EMM server can then mark the device as non-compliant and revoke access to corporate resources such as email, data storage, and VPN.

MAV evaluates the security of mobile applications to ensure that mobile apps conform to an organization’s security requirements and are reasonably free from vulnerabilities, and possibly assesses other issues including reliability, performance, and accessibility. Complementary solutions that integrate MAV tools with EMM and MTD can detect and defend against runtime security threats, often containing application vetting or similar services in conjunction with device and network level protections.

Network Monitoring is a passive feed of data from the Mobile Network Operators (MNOs) that should not interfere with existing capabilities and should enhance CISA’s situational awareness during event monitoring and inform tabletop exercises.

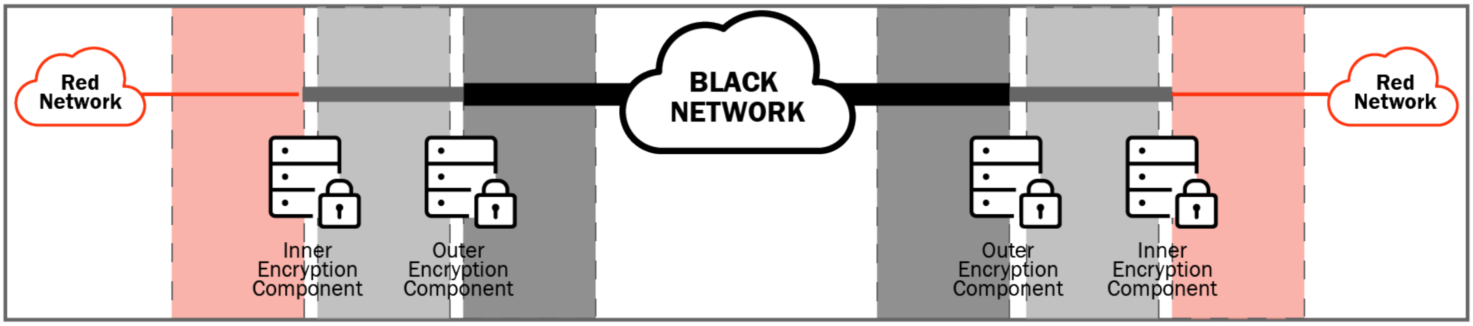
TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
MAV	ADOPT				
EMM and MTD	ADOPT				
Network Monitoring	ADOPT				

CISA should adopt these technologies internally and recommend adoption across the Federal, State, Local, Tribal, and Territorial (FSLTT) and critical infrastructure (CI) sectors to enhance the security (confidentiality, integrity, and availability) of smartphone stored data and communications.

Image Source: 42 Gears Team. (n.d.). Why Integration of Mobile Threat Defense (MTD) Solutions with EMM Makes Sense? Retrieved from https://www.42gears.com/white-papers/why-integration-of-mobile-threat-defense-solutions-with-emm-makes-sense/.

CELLULAR SECURITY

Commercial Solutions for Classified (CSfC)


Red Network
Inner Encryption Component
Outer Encryption Component
BLACK NETWORK
Outer Encryption Component
Inner Encryption Component
Red Network

The U.S. National Security Agency (NSA) developed and maintains a program, Commercial Solutions for Classified (CSfC), that leverages commercial encryption capabilities to provide adequate protection of classified data in an efficient and secure manner. The NSA's CSfC Program Management Office (PMO) publishes Capability Packages that specify how to layer commercial technologies for protecting National Security Systems (NSS) data.

The CSfC program is an alternative to Government-Off-the-Shelf (GOTS) type-one encryption devices. CSfC provides a mechanism to reduce or eliminate protected distribution systems in facilities and to reduce the amount of Controlled Cryptographic Items (CCI) in an organization. The CSfC program is founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications.

The CSfC capabilities are compatible with existing cellular network data services in use by national security and emergency preparedness (NS/EP), critical infrastructure (CI), and Federal, State, Local, Tribal, and Territorial (FSLTT) stakeholders. CSfC is an application layer set of capabilities that can be deployed on most versions of Apple and Samsung mobile devices.

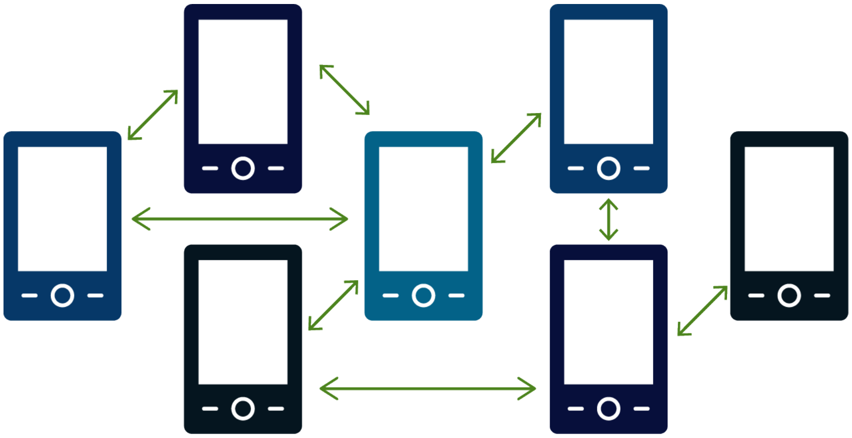
TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
DoD CSfC	ADOPT				

CISA should adopt CSfC for internal communications and recommend adoption across the NS/EP, FSLTT, and CI stakeholders.

Image Source: NSA. (2021, May). Cybersecurity Solutions. Multi-Site Connectivity Capability Package V1.1.8. Figure 1. Page 8.

CELLULAR SECURITY

Mobile Ad Hoc Network



Mobile Ad-hoc Network (MANET): A MANET is a collection of mobile nodes connected wirelessly that are dynamically and arbitrarily located, including interconnections between nodes that may change on a continual basis. A MANET may provide an optional regional alternative network capability if a Mobile Network Operator (MNO) or Land Mobile Radio (LMR) network is unavailable or experiencing a service degradation. A MANET may also provide benefits inside buildings or in adverse terrain where the wireless network may be operating properly but cannot reach the specific device location. The 3GPP has defined proximity-based (ProSe) services that may be able to support a MANET capability for smartphones.

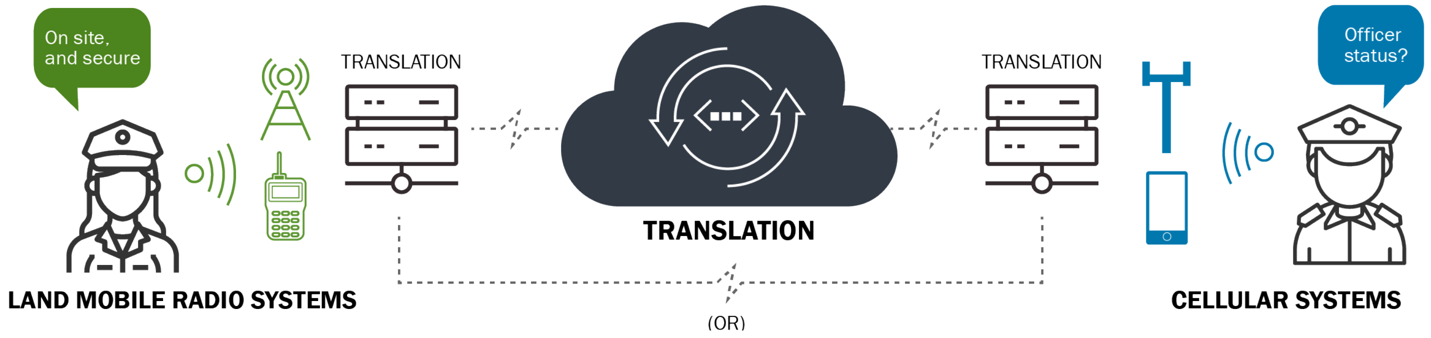
Each device in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. Additionally, each device must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

The MANET ad-hoc mobile networking capabilities can be deployed on existing mobile devices and should be considered a complement to cellular data networks as a capability to improve end-to-end (E2E) network resilience.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
MANET	ADOPT				

CISA should adopt these technologies internally and recommend adoption across the Federal, State, Local, Tribal, and Territorial (FSLTT) and critical infrastructure (CI) sectors. As part of this adoption, CISA could gather usage data of deployed devices regarding the effectiveness of MANET as a pilot project to maintain communications during incidents and the frequency of corrupt routing information to improve availability, confidentiality, integrity, authentication, and non-repudiation of MANET used by national security and emergency preparedness (NS/EP) stakeholders.

LAND MOBILE RADIO TO CELLULAR INTEROPERABILITY



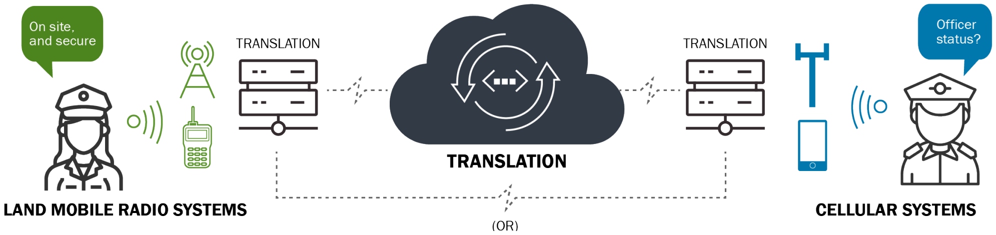
Land Mobile Radio (LMR) to cellular interoperability enables National Security and Emergency Preparedness (NS/EP) stakeholders and other Federal, State, Local, Tribal, and Territorial (FSLTT) stakeholders to establish cross-jurisdiction communications during planned and emergency events, missions, and exercises. The cellular (3GPP) standards for interoperability are under development at this time. However, industry recognized the need/opportunities for LMR to Cellular Interoperability and developed multiple proprietary interoperability solutions. Interoperability among the proprietary solutions has not been researched.

The proprietary solutions offer interoperability via cloud services that include a smartphone push-to-talk (PTT) app (voice over IP). In addition, multiple vendors offer LMR radios with built in data only smartphone capabilities to communicate via cellular data services to the vendor's cloud service. The service requires a separate connection to each subscribing jurisdiction's LMR system.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Cloud-based Cellular Interoperability	ADOPT				

CISA should recommend NS/EP and FSLTT operators adopt this technology to address LMR to Cellular interoperability gaps. CISA should also participate in on-going and future field studies and evaluations with the mobile network operators, other government agency (including DoD) efforts, and vendor efforts deploying LMR to Cellular interoperability capabilities. In addition, CISA should continue participating in the 3GPP specifications development and coordinate with other agencies, such as the National Security Agency (NSA) or National Institute of Standards and Technology (NIST), as well as government and private sector first responder communities of interest, to collect requirements and influence standards for the products and services that enable LMR to cellular interoperability.

MISSION CRITICAL VOICE ON CELLULAR NETWORK



Mission Critical Voice (MCV) capabilities have been identified as necessary for operations in a field environment by the National Public Safety Telecommunications Council. MCV needs require that user devices provide the following capabilities, which unmodified consumer smartphones do not provide:

- **Direct or Talk Around:** direct device-to-device communications
- **Push-to-Talk (PTT):** The speaker pushes a button on the radio and transmits the voice message to other units
- **Full Duplex Voice Systems:** simultaneously speak to and hear other users
- **Group Call:** equivalent to a conference call
- **Talker Identification:** equated to caller ID
- **Emergency Alerting:** highest priority queue position when needed
- **Audio Quality:** identify the speaker by their voice; detect stress in a speaker's voice; and hear background sounds from around the speaker, without interfering with primary voice communications

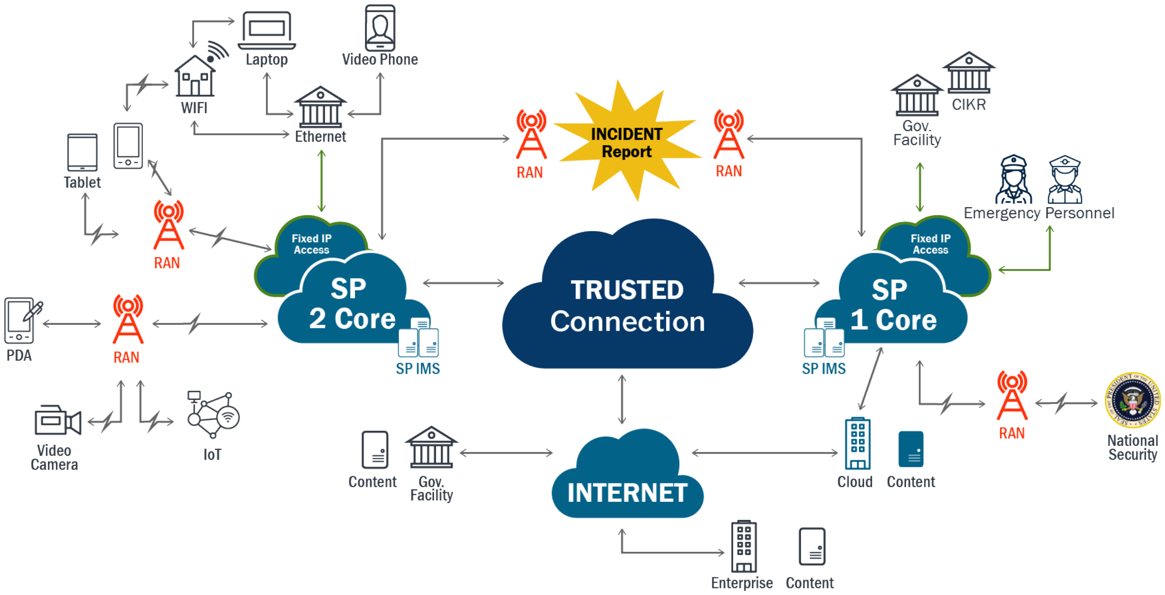
The 3GPP ProSe specification for device-to-device communications is intended for implementation within cellular devices. Combination LMR and cellular/smartphone devices are currently offered by multiple vendors. The MCV over cellular network service combines a PTT over-the-top (OTT) smartphone application, cloud-based voice service, cloud based LMR system interconnection, and the user organization's traditional LMR voice communications network to enable the service.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
ProSe device to device communications	ADOPT				
LMR/smartphone device integration	ADOPT				

CISA should recommend National Security and Emergency Preparedness (NS/EP) and Federal, State, Local, Tribal, and Territorial (FSLTT) users adopt this technology to address MCV on cellular networks. In addition, CISA should continue participating in the 3GPP specifications development and coordinate with other agencies, such as the National Security Agency (NSA) or the National Institute of Standards and Technology (NIST), that are participating in 3GPP MCV specifications development, as well as government and private sector first responder communities of interest, to collect requirements and influence standards for the products and services that enable MCV on cellular networks.

Image Source (FirstNet Device): FirstNet (n.d.). Device image. Retrieved from https://www.firstnet.com/mission-critical/firstnet-push-to-talk.html

NEXT GENERATION NETWORK PRIORITY SERVICES



5G: Fifth Generation
PDA: Personal Digital Assistant
IoT: Internet of Things
RAN: Radio Access Network

CIKR: Critical Infrastructure Key Resources
IMS: IP Multimedia Subsystem
SP: Service Provider

Next generation network (NGN) is the term used to describe the packet switched IP-based network supporting voice and data communications. NGN Priority Services (NGN-PS) will provide prioritized voice and data communications services for National Security and Emergency Preparedness (NS/EP) and Federal, State, Local, Tribal, and Territorial (FSLTT) users on both mobile (wireless) and terrestrial networks. NGN-PS also supports priority Short Message Service (SMS) and priority multimedia services (MMS) on mobile devices/user equipment.

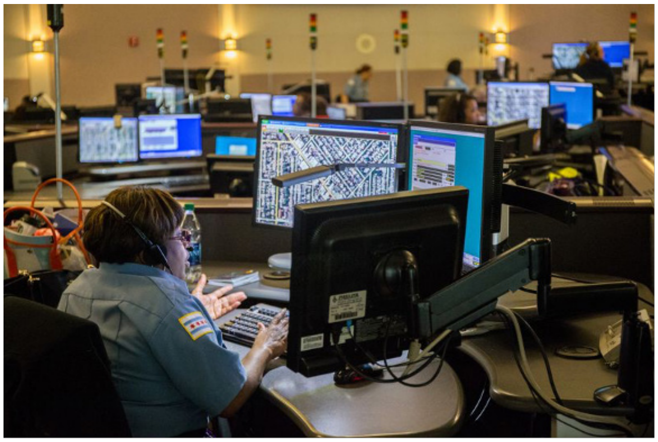
Many of the services/information sources utilized by CISA and their NS/EP stakeholders are hosted on networks outside the perimeter of the FSLTT network on which they are connected. Terrestrial network Internet service providers (ISP) (such as Verizon, AT&T, Cox) do not offer cross-ISP priority or pre-emption services.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
VPN service with proper QoS	DEMO				
Inter-ISP QoS	DEMO				
Government network peering	DEMO				
3GPP Priority and Pre-emption Specifications	MONITOR	DEMO			
Mobile Ad Hoc Network (MANET)	DEMO				

CISA should monitor and participate with other government organizations in the workgroups developing the 3GPP priority and pre-emption specifications. The four other technologies have the potential to support NGN-PS today and should be demonstrated in pilots or testbeds to illustrate their value to NS/EP and FSLTT organizations for priority services provisioning.

Image Source: DHS CISA, Billy Bobby Brown, J. N. (2020, April 9). Next Generation Network Priority Services (NGN PS) Phase 2: Data and Video Program Review. Retrieved May 25, 2020.

PUBLIC SAFETY ANSWERING POINT (PSAP) IMPROVEMENTS



NG911 technologies offer Public Safety Answering Points (PSAPs) the ability to accept data, share data with first responders, provide accurate location information, interconnect with other centers, provide mutual aid, and route vital services during emergencies.

Computer-Aided Dispatch (CAD) systems are used by Emergency Management Services to prioritize and record incident calls, identify the status and location of responders in the field, and effectively dispatch responder personnel. If PSAPs and Emergency Communication Centers have a resilient ability to interconnect CAD systems, there is potential to create an interoperable nationwide 911 system.

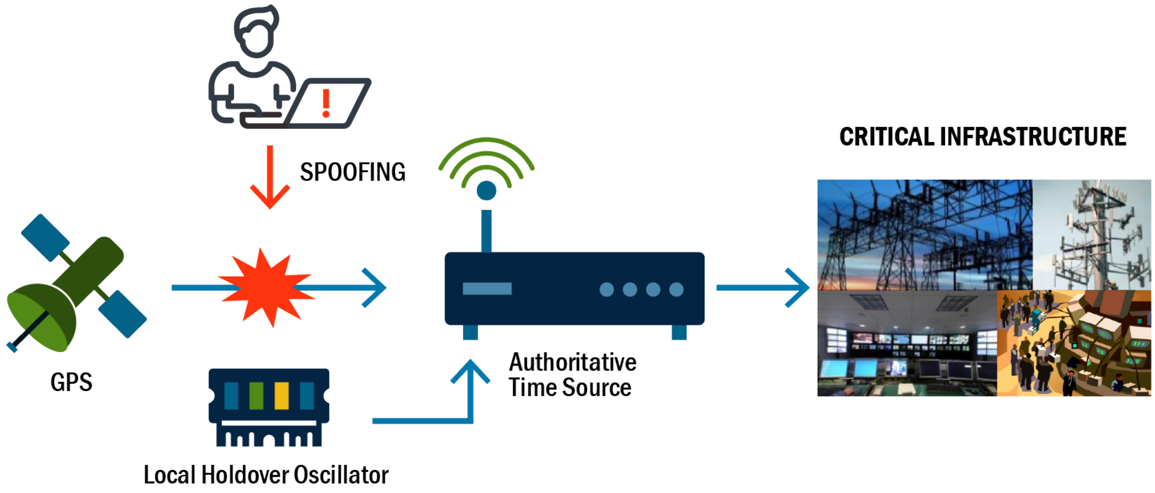
Precise location is the term used for technologies that provide highly accurate (within one meter) location (horizontal and vertical) detection and reporting indoors or outdoors. Current location services rely on Global Positioning System (GPS) based location capabilities which may be unavailable within buildings and wherever GPS signals are degraded (urban areas, subterranean locations). DHS components and first responders are interested in utilizing precise location capabilities to improve location tracking for improved situational awareness and user safety, and for tracking team members for incident command and common operational pictures.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
CAD Interoperability	ADOPT				
Precise Location and NG911 Higher Location Resolution	DEMO				

CAD-to-CAD interoperability is achievable today through activities for adoption of standards. CISA should seek to assist standards adoptions that facilitate interoperable CAD-to-CAD exchanges. CISA should work with precise location vendors and S&T Office of Interoperable Communications (OIC) to demonstrate implementations and determine the feasibility of accelerating deployment of precise location capabilities.

Image Source: Bzdak, Z. (2016, October 20). The 911 Call Center at the Office of Emergency Management and Communications (OEMC) in Chicago on Wednesday, March 30, 2016 [Chicago Tribune]. Retrieved from https://www.chicagotribune.com/politics/ct-city-budget-human-resources-met-20161019-story.html.

AUTHORITATIVE TIME SOURCE



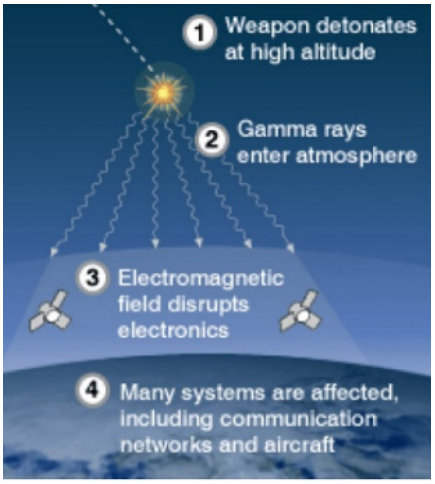
An authoritative time source is a single source of time (at a given local site) by which events can be time-stamped, correlated, and synchronized at a national and international level both for local and external use. Such a time source is necessary for efficient and effective cybersecurity operations (e.g., Security Orchestration, Automation, and Response; Security Information and Event Management; and forensic analyses). Additionally, functions and services executed at the local site depend on this time source for events such as timestamping financial transactions, controlling industrial plant operations, and synchronizing transmission media for communications. The authoritative time source is synchronized to Coordinated Universal Time (UTC) with an accuracy determined by the functions and services conducted at the local site (often at the microsecond level).

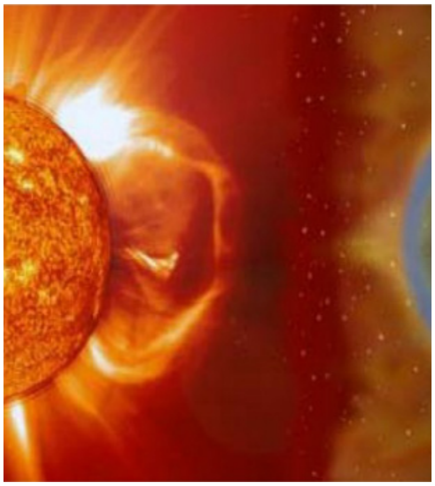
GPS is used broadly as a time source and has become the de facto national timing reference due to its ease of integration, precision, low cost, and wide availability. GPS, via the authoritative time source, provides the timing for functions executed within critical infrastructure (CI). GPS signals have low signal strength at the receiver and can be spoofed via various techniques. Active anti-GPS spoofing technology can detect these disruptions and protect the authoritative time source. Given the dependence on GPS, active anti-GPS Spoofing technology merits consideration as any disruption to the time source represents a major risk to communications systems, as well as many other CI sectors. Similarly, the ubiquitous need for a highly accurate timing source means that economically viable low-cost accurate atomic backup clocks must be available in the marketplace. These atomic oscillators are used to provide accurate time during periods when GPS disruptions are present (e.g., spoofing or interference).

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Active Anti-GPS Spoofing	ADOPT				
Low-Cost Accurate Atomic Backup Clock	R&D				

CISA should adopt active anti-GPS spoofing technology for internal usage and recommend to FSL
For the moment, CISA should maintain knowledge of DARPA and NIST progress in R&D efforts to develop low-cost atomic clocks with acceptable long-term drift rates. Once the capability is ready for a technology transfer to vendors, then CISA may elect to demonstrate the capability in pilots with various CI partners (or others).

ELECTROMAGNETIC PULSE (EMP) AND GEOMAGNETIC DISTURBANCE (GMD) MITIGATIONS


1 Weapon detonates at high altitude
2 Gamma rays enter atmosphere
3 Electromagnetic field disrupts electronics
4 Many systems are affected, including communication networks and aircraft



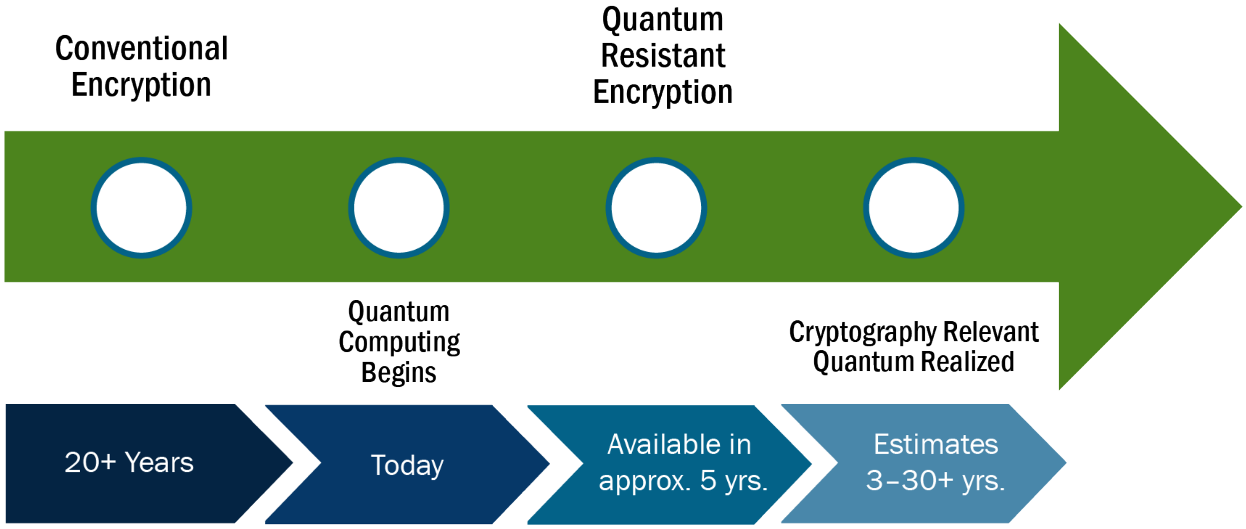
An electromagnetic pulse (EMP) is a burst of electromagnetic energy that has the potential to negatively affect technology systems on Earth and in space. A high-altitude EMP (HEMP) is a type of human-made EMP that occurs when a nuclear device is detonated at approximately 40 kilometers or more above the surface of the Earth. A geomagnetic disturbance (GMD) is a natural EMP due to a temporary disturbance of the Earth's magnetic field resulting from a Coronal Mass Ejection (CME). Both HEMPs and GMDs can affect large geographic areas. The effects of any of these electromagnetic disturbances are of national concern for all CI sectors, including destruction of unprotected electronics in communications systems and adverse effects on the electric grid. These effects can be mitigated via passive or active technologies. Passive technologies (e.g., resistors and capacitors installed on transmission lines, surge arresters, Faraday cages, and grounding) are installed in infrastructure at all times, while active technologies are switched into place when an event is detected.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Passive EMP/GMD Mitigation Technologies and Techniques	ADOPT				
Active EMP/GMD Mitigation Technologies and Techniques	R&D				

Because mitigation technologies are available, the lack of adoption of EMP mitigation technologies is the result of other causes. CISA should adopt passive EMP mitigation where appropriate and cost effective (e.g., high value asset data centers and command/operations centers). CISA should strongly recommend to CI (particularly the electric generation and transmission industry, and the communications sector) to adopt passive EMP mitigations, especially for an E3 pulse (late-time, low-amplitude, long-duration pulse). CISA should track industry R&D efforts for active EMP mitigations until availability is higher. Furthermore, CISA should work with DOE and FERC to develop EMP/GMD guidelines for the bulk power system.

Image Source: Pugh, S. (2012). Extreme Space Weather (ESW) and EMP, Comparisons and Contrasts. DHS S&T.

QUANTUM RESISTANT ENCRYPTION


Conventional Encryption
Quantum Resistant Encryption
Quantum Computing Begins
Cryptography Relevant Quantum Realized
20+ Years
Today
Available in approx. 5 yrs.
Estimates 3–30+ yrs.

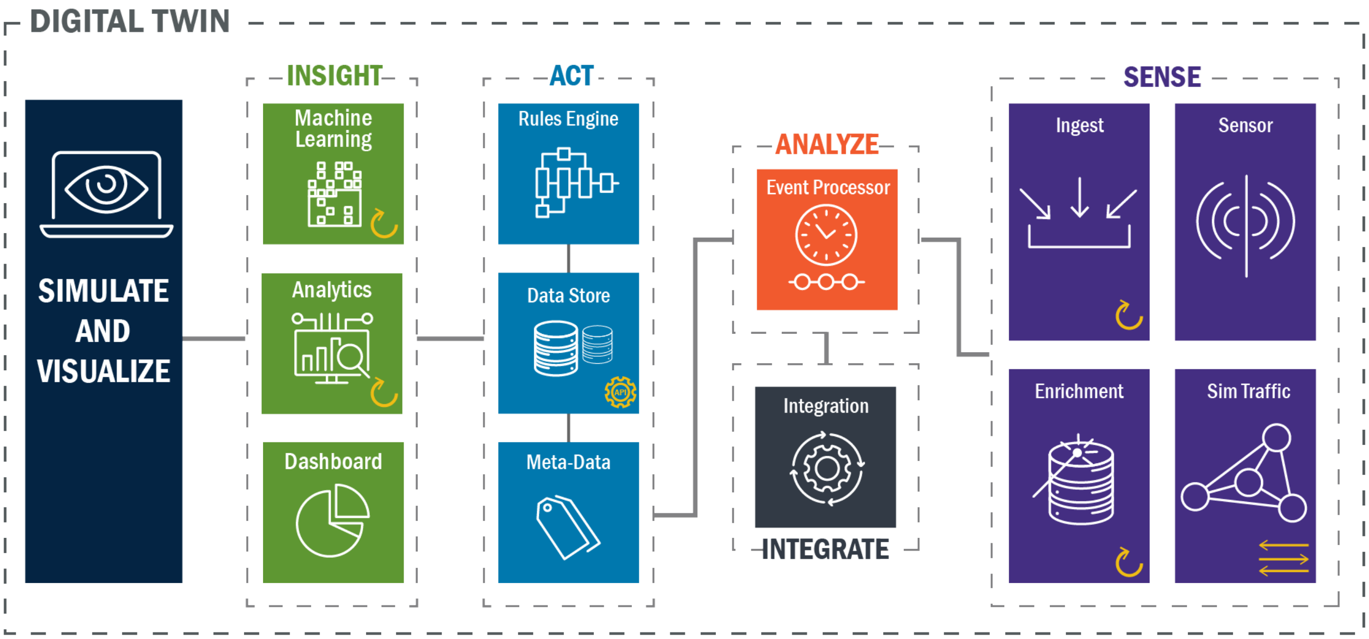
Quantum Resistant Encryption (QRE) is the next generation of encryption algorithms designed to be secure against both quantum and classical computers yet remain compatible with existing communications protocols and networks. The first generation of quantum computing (QC) able to reliably implement the algorithms necessary to break the asymmetric encryption used in today's public key cryptography/infrastructure (PKC/PKI) is termed a cryptography relevant quantum computer (CRQC). QRE is a requirement for security when CRQCs are realized. Crypto agile encryption (CAE) is the recommended approach to achieve QRE. CAE is an enhancement to enable future encryption algorithm changes without operational disruptions such as those expected for the QRE transition.

The security risks that a CRQC creates include the loss of confidentiality and integrity of data at rest and data in transit. The security risks also include the loss of integrity of the authentication mechanisms used for access and permission decisions on virtually all enterprise and public Internet applications and services. In addition, integrity of software distribution techniques is reduced or eliminated due to the use of PKI for integrity checks.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Crypto Agile Encryption	R&D				

CISA should track NIST standards efforts and industry R&D efforts to develop QRE. CISA should plan to kick-off adoption activities approximately 4 years from the date of the STR. Given the time required to transition (up to a decade), the transition planning should begin now. CISA should also recommend to acquisition organizations within CISA; the Federal, State, Local, Tribal, and Territorial (FSLTT) entities; and critical infrastructure (CI) that they initiate discussions and approaches to include QRE requirements in acquisitions as soon as feasible. Given the near-term time when NIST-approved CAE algorithms are available, considering these CAE algorithms in acquisitions should start now. The acknowledgment of the coming era of CRQC across government, CIs, and industry is needed to maximize the probability that the capabilities will be available when needed.

RISK REDUCTION VIA MODELING (DIGITAL TWIN)



Modeling is often used to reduce risk in system development, operations, and planning. A digital twin is a specific type of model that is a virtual representation of real-world items (systems, production plants, power grid) and processes that is synchronized with its real-world counterpart at a specified frequency and fidelity. They do not replace other modeling and simulation or laboratory experimentation but are a value-added capability. Benefits include improving efficiency, limiting downtime, managing risks, planning upgrades, supporting what-if analysis, and simulating cyber-attack scenarios.

Digital twin technology can create a platform for better and consistent situational awareness. By closing the loop between operations, engineering, environmental factors, and threat information, digital twins can deliver meaningful, actionable insights with powerful visualizations of risk and operational activity.

A goal of digital twins is to facilitate real-time analysis as opposed to low fidelity, historic, or static models, which do not use real-time parameters. Since a digital twin is constantly being updated with information from its real-world counterpart, it is uniquely positioned to learn and monitor concurrently, can perform predictive analysis, and test changes to processes, services, and configurations.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
Digital Twin	ADOPT				

CISA should invest in digital twins within its mission space as an additional tool for reducing risks and to gain insight, experience, and credibility to influence approaches that would continue evolution of digital twin platforms. CISA should encourage the use of digital twins among critical infrastructure stakeholders. CISA should also consider involvement in industry and standards organizations, such as the Digital Twin Consortium, to influence approaches that would underpin the continued evolution of digital twin platforms.

Image Source: Draft CISA Target Architecture v1.

5G AND INTERNET OF THINGS SITUATIONAL AWARENESS FOR OPERATIONS CENTERS

The advent of 5G and Internet of Things (IoT) provides an opportunity for increasing the scale and quality of sensor data used by operations centers to develop situational awareness within their mission space, as well as reducing latency in receiving sensor inputs.

Subject to applicable law, U.S. Government and industry should develop methods to effectively characterize "normal/healthy" conditions versus "suspicious/unhealthy" 5G and IoT environments. Without sufficient situational awareness, personnel and systems could suffer cyber-attacks (such as disrupting an IoT medical device or transportation system) utilizing undetected exploits that leave no trace of the attack vector. Development of a robust 5G and IoT Situational Awareness System (5i SAS) capability that preserves privacy and civil liberties, can help ensure safety and security. 5G devices have embedded sensors that can detect bio activities, sounds, video, and electromagnetic activity and can interact with IoT sensors to monitor a wide range of environmental data.

A comprehensive 5i SAS should enable informed decision making about network and device security and resilience. It would incorporate Distributed Sensor Data via 5G and IoT and provide the following capabilities: IoT Device Management, Automated Data Collection, IoT Sensing and Data Collection, Packet Storage, User Plane Processing, Control Plane Processing, Threat Intelligence and Analysis, Dependency and Impact Analysis, and Analysis of Alternatives.

Situational awareness is important for decision making to ensure that there is sufficient perception of the elements within the operating environment, comprehension of their meaning, and projection of their status in the future.

TECHNOLOGY	< 2 YRS	2-3 YRS	3-4 YRS	4-5 YRS	> 5 YRS
5G and IoT Situational Awareness for Operations Centers	ADOPT				

It is recommended that CISA acquire lawful IoT and 5G monitoring capabilities to gain necessary situational awareness.

Image Source: Tierney, M.J. (n.d.). 5G network with downtown Los Angeles at night [Royalty-free stock photo ID: 1349472458]. https://www.shutterstock.com/image-photo/5g-network-downtown-los-angeles-night-1349472458.

CAPABILITY FORECAST: DHS S&T, NSF, AND ONR

R&D Project Mapping to Capability Demand Areas

R&D PROJECTS

		CYBERSECURITY								COMMS				CRITICAL ENABLERS					
		ICS Security	IoT Security	Large Scale Analytics	Network Systems Security and Resilience	Resilient Machine Learning Systems	SOAR Effectiveness	Software Assurance and Vulnerability Mgmt	Vehicle Security	Cellular Security	LMR to Cellular Interoperability	Mission Critical Voice on Cellular Networks	Next Generation Network Priority Services	Public Safety Access Point Improvements	Authoritative Time Source	EMP and GMD Mitigations	Quantum Resistant Encryption	Risk Reduction via Modeling	Situational Awareness (via 5G and IoT)
DHS S&T	Cyber Analytics and Platform Capabilities				●		●												
	Cybersecurity Innovation Laboratory (CyLab)			●	●		●												
	Electromagnetic Pulse (EMP) and Geo-Magnetic Disturbance (GMP) Resilience															●			
	Emergency Communications												●	●					
	GPS Vulnerability for Critical Infrastructure														●				
	Joint Analytics Collaborative Environment (JACE)			●	●		●												
	Qubit																●		
	Secure and Resilient Mobile Network Infrastructure (SRMNI)									●	●	●							
	Software Assurance							●											
NSF	Decentralized Internet Access Management System - Post-Quantum Security				●														
	Linking2Source: Security of In-Vehicle Networks via Source Identification								●										
	Specifying and Verifying Secure Compilation of C Code to Tagged Hardware							●											
	Using Machine Learning to Build More Resilient and Transparent Computer Systems			●		●													
ONR	RHIMES							●											
	Total Platform Cyber Protection (TPCP)							●											
	TOTAL (24)	0	0	3	4	1	3	4	1	1	1	1	1	1	1	1	1	0	0

CAPABILITY FORECAST: DARPA

DARPA Project Mapping to Capability Demand Areas

	R&D PROJECTS	CYBERSECURITY								COMMS					CRITICAL ENABLERS				
		ICS Security	IoT Security	Large Scale Analytics	Network Systems Security and Resilience	Resilient Machine Learning Systems	SOAR Effectiveness	Software Assurance and Vulnerability Mgmt	Vehicle Security	Cellular Security	LMR to Cellular Interoperability	Mission Critical Voice on Cellular Networks	Next Generation Network Priority Services	Public Safety Access Point Improvements	Authoritative Time Source	EMP and GMD Mitigations	Quantum Resistant Encryption	Risk Reduction via Modeling	Situational Awareness (via 5G and IoT)
DARPA	Artificial Intelligence Mitigations of Emergent Execution (AIMEE)							●											
	Assured Micropatching (AMP)	●							●										
	Atomic Clock with Enhanced Stability (ACES)														●				
	Automatic Implementation of Secure Silicon (AISS)							●											
	Automated Rapid Certification Of Software (ARCOS)							●											
	Computers and Humans Exploring Software Security (CHESS)							●											
	Data-Driven Discovery of Models (D3M)																	●	
	Data Protection in Virtual Environments (DPRIVE)			●													●		
	Explainable Artificial Intelligence (XAI)			●			●												
	Extreme DDoS Defense (XD3)				●														
	Open, Programmable, Secure 5G (OPS-5G)									●									
	Reverse Engineering of Deceptions (RED)					●													
	SAFEWARE							●											
	Verified Security and Performance Enhancement of Large Legacy Software							●											
	TOTAL (17)	1	0	2	1	1	1	6	1	1	0	0	0	0	1	0	1	1	0

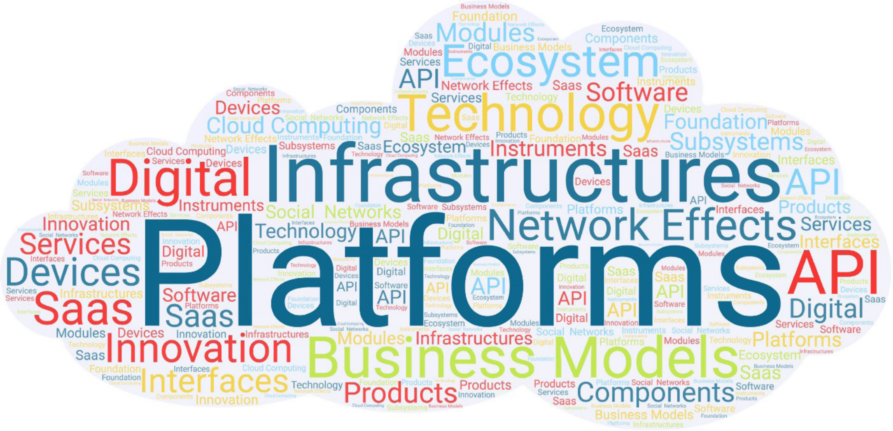
CAPABILITY FORECAST: DOE

DOE Project Mapping to Capability Demand Areas

R&D PROJECTS

		CYBERSECURITY								COMMS					CRITICAL ENABLERS				
		ICS Security	IoT Security	Large Scale Analytics	Network Systems Security and Resilience	Resilient Machine Learning Systems	SOAR Effectiveness	Software Assurance and Vulnerability Mgmt	Vehicle Security	Cellular Security	LMR to Cellular Interoperability	Mission Critical Voice on Cellular Networks	Next Generation Network Priority Services	Public Safety Access Point Improvements	Authoritative Time Source	EMP and GMD Mitigations	Quantum Resistant Encryption	Risk Reduction via Modeling	Situational Awareness (via 5G and IoT)
DOE	Assessment of Usability of ML Based Tools for the Security Operations Center						●												
	Data-Driven Model Generation For Deception Defense Of Cyber-Physical Environments	●			●														
	Industrial Control Systems Network Protocol Parsers	●																	
	Review of Intrusion Detection Methods and Tools for Distributed Energy Resources	●	●																
	Time-Based CAN Intrusion Detection Benchmark								●										
	Toward an Electromagnetic Event Resilient Grid															●			
	Cybersecurity Intrusion Detection and Security Monitoring for Field Area Networks	●																	
	Detection and Analysis of Threats to the Energy Sector (DATES)	●																	
	Hallmark Cryptographic Serial Communication	●																	
	Patch and Update Management Program for Energy Delivery Systems	●																	
	Secure Information Exchange Gateway for Electric Grid Operations (Siegate)	●																	
	Software Defined Networking (SDN) - Energy Sector	●																	
	Tempus Project Time Synchronization Platform for GPS Spoofing														●				
	Timing Intrusion Management Ensuring Resiliency (TIMER)														●				
	Watchdog	●																	
	TOTAL (17)	10	1	0	1	0	1	0	1	0	0	0	0	0	2	1	0	0	0

PLATFORM WEAPONIZATION



Platforms establish and deepen connections between people spanning all forms of transactions, personal relationships, information exchanges, and the development and spread of new ideas. Our virtual ecosystems exist because of platforms, yet their nature and complexity elude understanding. Complex interactions of actors on platforms can exhibit “emergent behavior.” Emergent behavior describes outcomes and effects that “cannot be predicted through analysis at any level simpler than that of the system as a whole,” (Dyson, 1997). The exchanges that occur on platforms can manifest real-world consequences such as election interference, stock market manipulation, and spreading of false narratives and misinformation such as COVID-19 vaccine efficacy.

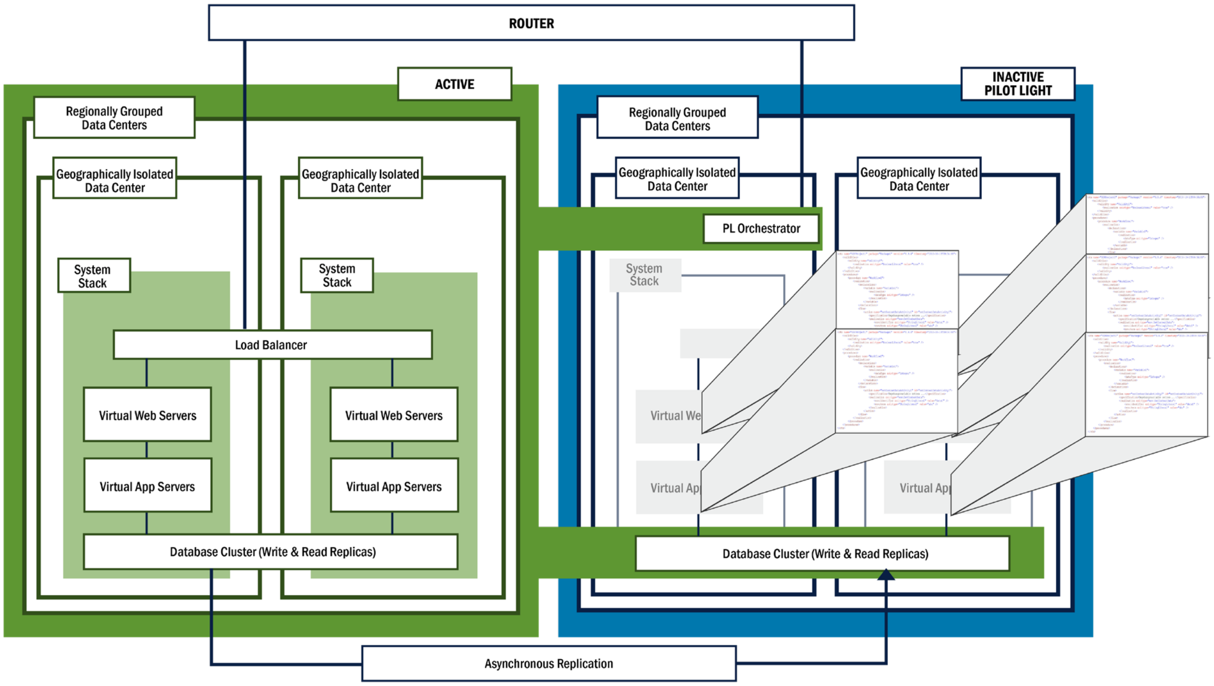
An adversary can weaponize a platform by exploiting emergent behaviors. The potential to use emergent behaviors for nefarious purposes necessitates rethinking of traditional technology risk management. We can no longer simply apply security controls to mitigate against known vulnerabilities and exploits. Adversaries can potentially weaponize platforms even when the platform is working as expected and there are no information breaches. Platform weaponization can

1. Infringe on the rights of people;
2. Unlawfully target groups, industries, individuals; or
3. Create financial, economic, political, and other problems.

Platform weaponization potentially will become increasingly prevalent and complex, and it will likely threaten democratic processes, commerce, markets, and trust in institutions. Attacks from weaponized platforms will be difficult to identify, contain, and remediate based on the speed and scale at which they will occur. CISA needs to start preparing for such attacks by considering and developing stronger capabilities to identify and manage risks of which we are not aware and do not understand.

Image Source: Kolossovski. (2019). A strategist’s guide to platform thinking.

INFRASTRUCTURE AS CODE AND PILOT LIGHT (ICPL) FOR AGENCY-LEVEL RECOVERY FROM DEEP COMPROMISE


ROUTER
ACTIVE
INACTIVE PILOT LIGHT
Regionally Grouped Data Centers
Geographically Isolated Data Center
Geographically Isolated Data Center
System Stack
System Stack
Load Balancer
Virtual Web Servers
Virtual Web Servers
Virtual App Servers
Virtual App Servers
Database Cluster (Write & Read Replicas)
Regionally Grouped Data Centers
Geographically Isolated Data Center
Geographically Isolated Data Center
PL Orchestrator
System Stack
Virtual We
Virtual Ap
Virtual Ap
Database Cluster (Write & Read Replicas)
Asynchronous Replication

An active SolarWinds-style compromise erodes trust in the integrity of an agency's infrastructure, communications, and data (collectively, the system), and this erosion is exacerbated by the possibility that an adversary has access to communications about remediation actions and other sensitive operational data. During remediation, an agency may operate an out-of-band communications infrastructure, allowing for critical operational coordination between leaders and infrastructure engineers; however, that solution only helps to remove the adversary from the remediation planning and communications loop. Forensic preservation and adversary containment compete for finite resources when restore point and time objectives (RPO and RTO) are invoked during disaster recovery (DR) scenarios. Conversely, RPO and RTO that would otherwise be expected in 10s of minutes or hours may be pushed into days, weeks, or months while the compromise is investigated, forensics collected, and remediation actions planned and executed. With out-of-band communications focused on forensics and remediation planning, in-band operations are minimized or frozen to prevent continued leakage of operational data further impacting operational capabilities.

Infrastructure as Code and Pilot Light (ICPL) may offer a means for detaching, freezing, and preserving the compromised system while instantiating a new uncompromised system within or near RPO and RTO; however, to realize this concept, the system must be codable (a scripted version of the system), data must be asynchronous (asynchronous records minutes after a transaction, not hours or days), and CSP infrastructure must be reserved and on standby with immediately scalable capacity. Solving the ICPL problem lays the groundwork for future innovations such as Authority to Operate (ATO) of Infrastructure as Code (IaC), as the code is a replica of the operational environment. That could reduce ATO to seconds. ATO remediations can be applied to system code, which in turn is deployed to the operational environment.

The current state of ICPL technology does not scale to agency-level IaC reconstitution where all systems (voice, network, compute, data) can exist and restore from code within RPO and RTO while detaching, freezing, and preserving the compromised system. ICPL at scale requires the availability of reserved capacity to instantiate agency instances across multiple CSPs and it requires the technology capability to facilitate full codification of the system and end-user compute environments. When ICPL transitions from speculative to feasible, for the Federal Government, its use as a DR strategy and for major cybersecurity incident handling will require new authorities, coordination, and processes.

DEFINITIONS FOR CAPABILITY DEMANDS FINDINGS AND RECOMMENDATIONS TABLES

ADOPT: CISA concludes that CI industry and/or government (internal CISA and/or FSLTT) should adopt, or encourage adoption of, a technology or capability. The Adopt phase is focused on operationalizing a new technology, such as developing and utilizing deployment best practices, infrastructure integration and delivery, operational procedures, external relationship management, and human resource development.

DEMONSTRATE: These items have seen sufficient R&D investment to consider worth pursuing to understand how to improve the capability and incorporate it into the operations of a stakeholder or project that can tolerate the risk (e.g., pilot, prototype, testbed, large-scale experiment). The Demonstrate phase is focused on ensuring that the value proposition can be maintained while the deployment risk is managed in order to justify operational integration.

R&D: These items show significant value potential for improving operations or mission effectiveness and are currently, or should be, planned for R&D investment (e.g., lab breadboards or experimentation, R&D funding for applied research). The R&D phase is designed to "stabilize" an emerging technology, which may include experimentation, hiring of engineering resources, and developing a strategy for integrating an emerging technology into operational capabilities. Items recommended for R&D have moved beyond the conceptual to the growth phase, where the emerging technology must be exploited to further understand the development and integration challenges, value proposition, and risk factors.

MONITOR: These items are identified as worth considering with the goal of understanding how they might affect CISA and stakeholder operations and/or improve mission effectiveness, to justify further R&D or other investment in the future. Monitor items may include elements that are still conceptual in nature and require evolution prior to further investment, experimentation, and potentially adoption. The Monitor phase is focused on identifying those technologies that show potential for significant value proposition and capacity to significantly alter or disrupt how essential mission functions are executed in the future. Monitor items may have uncertainty around the risks the technology poses due to maturity, state of R&D, and complexity.