# Cybersecurity


2020

2021-2022

2023-2024

2025+

Reliance on passwords, pass phrases, and SMS based authentication (MFA) is proving insufficient. The future will rely on multi-factor authentication coupled with behavioral heuristics that allow anomaly detection of fraudulent activity. MFA based on trusted devices – think mobile devices from Apple and Android that are known to service providers – coupled with machine learning and other artificial intelligence tools to apply behavioral analysis is needed to combat phishing and social engineering. The same techniques used for consumers will be applied to company insiders, a necessary step to achieving a zero-trust model.

Development Operations has already transformed service development and delivery. sScuring the development environment, much less the service delivery chain, has lagged core development activities. This is changing as security is integrated into the DevOps culture, commonly described as Development Operations Security (DevSecOps). While the press is largely focused on cultural aspects of DevSecOps, technology evolution is part of the picture, too. Providence of code, cyber supply chain management, integrated security testing, use of pervasive identity and authentication throughout continuous integration and delivery but also development must be supported.

Piracy and counterfeiting of physical and digital assets continue to plague distribution ecosystems. This is a common problem for music, prose, and video media, costing the industry billions. While law enforcement efforts strive to address the challenge, the core issues are technical and social. Who created what, who owns what, who can use what? On the technical front, content and material fingerprinting technologies are trying to provide a root of trust for provenance, proving definitively the original creator or manufacturer of cyber or physical media. Distributed ledgers will be used to publish fingerprints or signatures of new items in public blockchains to aid in ensuring provenance.

The two core protocols that make the internet work, DNS and Border Gateway Protocol (BGP), are under continually under attack and at risk of being hijacked. For example, attacks may cause BGP to route IP addresses differently (sometimes just detouring the route, sometimes changing the end point). Or attacks may change the authoritative resolution of DNS domains to different IPs, resulting in web traffic going to different sites than the user thought they were going to. Several competing approaches are being investigated to secure BGP and DNS. There will be convergence, but there may be significant technological and societal disruption in the interim.

Supply chain security has become a major focus of U.S. government regulator's attention working to ensure providers of government infrastructure know where the hardware and software they use come from. As a result, new and improved tools and controls for supply chain risk management have emerged including blockchain or similar registration processes to track physical and digital asset providence. Tamper resistant /proof mechanisms will be incorporated into hardware and software to protect serial numbers and prove providence. Automated scanning of software will continue to improve and be incorporated into DevOps and similar processes to ensure that software includes only elements that are expected and to identify unsafe code.

The usefulness of networked devices is dependent on having open interfaces to connect to networks. It's hard to know how to protect a device without knowing something about those interfaces. One solution under development in the industry is the IETF's Manufacturer Usage Description (IETF RFC 8520); but this approach probably won't address the longer-term industry needs. Profile based security solutions will emerge which leverage a profile for a user or device so that cyber security solutions will know how best to assure the desired experience. These profiles can also transform the user experience by making AI based anomaly detection more effective and support more comprehensive policy-based security and network decisions.

The (Wi-Fi Alliance) WFA and (Open Connectivity Foundation) OCF are working to streamline the on-boarding of IoT devices on Wi-Fi networks. The goal is ensuring that users stay in control of their networks. This requires ecosystem engagement across vendors, operators, and open source code groups (like the Linux Foundation). The WFA's EasyConnect ™ specification and OCF's Onboarding specification will need to be incorporated into silicon over the next two or three years and supported by operators to complete the transformation.

Adversaries attacks and network architectures are continuously evolving which requires our network's security posture to adapt quickly. Processes exist for updating the signatures on firewalls and Internet protection software on endpoints, and lots of end point devices (including mobile devices) are automatically patched. Ensuring that security tools deployed on access and premise networks can adaptively respond to attacks is the next step. The goal is a security posture that is harder for adversaries to track and subvert and improved economics as companies employ only the security that is necessary to deal with actual threats. Virtualization is the key enabling technology and will allow security software to be dynamically deployed where and when needed to detect attacks, mitigate them, and then remove or isolate infected devices.

As the owner and the creator of your own private info you will have control over its lifecycle: termination, erasure, and visibility into when, where, how it's to used. The EU has broadly adopted GDPR and California passed one of the toughest data privacy laws which went live in 2020 (California Consumer Privacy Act of 2018). With self-sovereign identity, individuals don't rely on another party, such as Facebook, to issue them an identifier for their use. They create the identifiers and own and control them along with what information is shared with whom under what conditions.

Just as AI can be used for cyber-defense, it can be weaponized for offensive purposes.  Hackers ability to launch sophisticated automated AI based attacks will grow, AI/Machine Learning helps to identify real time threats but also enable s hackers to carry out more sophisticated attacks. It's the Electronic Counter Measures and Electronic Counter/Counter Measures (ECM/ECCM) cycle.

Agile security architectures are not enough to keep pace of our adversaries. The ability to reprogram and update our security solutions along with security tools that benefit from cryptography, quantum resistant algorithms, and light weight cipher algorithms will be necessary. The ability to employ these advances without expensive and disruptive changes to access network architectures is an economic necessity requiring programmable security mechanisms (software and hardware) that can adapt to new threats and enable new capabilities without replacing infrastructure.

Phishing and other social engineering attacks continue to be employed in most successful cyber-attacks today. Adversaries use these mechanisms to directly execute fraud or to gain access to or change credentials so they can execute other attacks (such as deploying ransomware on key servers at a business). The intersection of big data and artificial agents (such as Cortana, Alexa, or MyCroft) will give rise to more advanced agents that can help detect fraudulent calls and emails much more effectively than a person can.

Trusted execution environments provide the ability to execute code on a server that is resistant to introspection or other types of attacks possible on virtualized environment. Major chip manufacturers have developed proprietary solutions. As software-based architectures become even more widely deployed, use of trusted execution environment technology will evolve. Standard instruction sets that ensure cross-platform support will transform the ability of service providers to secure virtual services.

Quantum key distribution (QKD) can, in principle, offer information-theoretical security between two remote parties, guaranteed by the fundamental laws of quantum mechanics. This is because eavesdropping on a quantum information channel destroys the state being transmitted, and thus can be detected by the parties involved. QKD is important because early prototypes of quantum computers, employing quantum algorithms, can in principle factor very large numbers and threaten current cryptosystems.

Significant research continues the use of classical approaches (methods that do not rely on quantum technology) to achieve quantum resistant cryptography. Research on solutions that are resistant to Shor's and Grover's quantum algorithms are promising. NIST is considering solutions (in fact, they are currently considering 26 distinct algorithms) for post-quantum cryptography. It's likely to take at least five years to complete the process for these algorithms to become available to the industry at large.