APPROIVED FOR DISTRIBUTION A
43-9050-22
20 JAN 2022

TECHNOLOGY TRENDS AND IMPACT ON CYBER BATTLEGROUND

A Cyber CoI Study

ABSTRACT

This report documents the findings of a study conducted by the DoD Reliance 21 Cyber CoI to identity and research technology trends that could have major impact on the cyber battleground, and thus may shape the future science and technology efforts. Simply stated, the goal of the study is to understand the future now so the DoD can better prepare for tomorrow.

Core Study Team and Authors:
Lead: Bharat Doshi
Other core team members: Emmanuel Bello-Ogunu, Adam Cardinal-Stakenas, Daniel Clouse, Ryan Craven, Joshua Jenks, Robert Kimball, Alexander Kott, Marc Lovend, Joseph Mathews, Paul Robb

Acknowledgments:
Alexandra Landsberg, Cyber CoI Lead, provided extensive guidance during the course of this study

Giorgio Bertoli provided the impetus to the study when he was the Cyber CoI Lead.

Chad Heitzenrater provided valuable and detailed comments on an earlier draft.

Technology Trends and Cyber Battleground: A Cyber CoI Study

Table of Content

1 Executive Summary

1.1 Background and Scope of the Study

Cyberspace technologies move quickly. 25 years ago, Google didn't exist. Just 15 years ago, it was unclear why a phone would ever need to do anything besides call and text, and clouds only existed in the sky. While the innovations in cyberspace technologies have provided major gains in personal and professional lives, they have also introduced vulnerabilities that have been exploited with increasing degree of sophistication and severity of consequences. Over the last three decades, cyber-attacks have gone from clever hacks shared among curious hobbyists to a complex, public battleground with a wide range of impacts: from impeding an adversarial nation-state's pursuit of nuclear weapons, to casting doubt on free and fair elections, to criminal groups extracting ransoms from desperate hospitals, pipelines, and municipal governments that have been prevented from functioning. Defense and exploitation of ever-changing and expanding cyberspace presence is now a full-fledged academic discipline, subject of science and technology (S&T) endeavor in industry and Government, and a warfighting domain with its own Combatant Command. Changes in cyberspace technologies and their expanding applications shape the cyber battleground and create new challenges for Cyber S&T. The rapid pace of these changes brings unique challenges to long-term planning of Cyber S&T. A well-known statistician, George Box, once said, "All models are wrong, but some are useful". The same applies to technology projections. No one can honestly say they know exactly what the next 20 years holds for cyberspace technologies and their applications, but the projections generated using informed sources and a well-executed process could provide valuable input to S&T planning.

Understanding relevant technology trends and projecting their impacts on the cyber battleground is the key goal of a study conducted by the DoD's Reliance 21 Cyber Community of Interest (CoI) over the course of several months in late 2020 and early 2021. This report documents the findings of that study. As part of the external input to the study, the CoI consulted many organizations with broad research and development agendas as well as over 100 diverse experts from across industry, academia, Government, Federally Funded Research and Development Centers (FFRDCs), and University Affiliated Research Centers (UARCs) through a series of surveys and interviews. To better understand the full range of forces that might impact the cyber S&T needs, this diverse pool of expertise contained many voices outside of the traditional cyber defense expertise, including artificial intelligence (AI), machine learning (ML), quantum science, microelectronics, and across the field of computing and networking at large. Their assessments, opinions, and predictions about the future of relevant technologies were pulled together and interpreted by the study team into a holistic, complete, and well-informed assessment describing the major changes likely to impact the future cyber battleground. The scope of this study is broad, but its goal is straightforward**:** ***understand the future now so the DoD can best prepare for tomorrow.***

1.2 Key Technology Trends

The study identified broad trends in groups of cyberspace technologies as well as specific trends in individual technologies. Some of the trends discussed below and the strength of their impacts seem relatively easy to anticipate using extrapolations of the histories of relevant technologies. Some other trends and/or their impacts were not quite as easy to anticipate, and they need special attention. Among the broad trends, increasing automation, complexity, programmability, virtualization, and opacity of supply chain is one set of such trends. They influence almost all cyberspace technologies and their applications, supply chains, and required reaction times. The second set arises from the increasingly tighter relationships between various cyberspace technologies (e.g., cyber and ML, each consisting of multiple technologies) and between cyberspace technologies and application areas (e.g., cyber and physical). These tight relationships requite interdisciplinary S&T focused on the challenges and opportunities at their intersections. Among technology specific trends, microelectronics, Internet of Things (IoT), (semi)-autonomous platforms, digital persona, and ML are likely to have major influence on the cyber battleground. On the applications side, the confluence of low SWaP-C (size, weight, power, and cost) IoT sensors, increasing networking speed, and advancement in computing will accelerate the use of data driven control in all critical infrastructures, mobile platforms, weapons systems, healthcare, and robotics. This rapid transformation of physical systems into smart cyber-physical systems (CPS) will lead to improved performance and automation, while adding new vulnerabilities. Integration of inorganic (cyber and physical) with organic (bio and neuro) will lead to a fundamental shift in the cyber battleground as well as the human-machine teaming techniques.

The trends are discussed below in two groups. The first group includes broad trends, each involving multiple cyberspace technologies and the ecosystem of their development, delivery, and use. The second group discusses trends in each of the important cyberspace technologies individually.

Broad Trends, Each Involving Multiple Technologies as well as Their Development, Delivery, and Use

Curse of complexity*:*

The increased scale and complexity of IT systems will create the biggest impact on cyber security and operations over the next 25 years. We cannot maintain technical superiority while continuing to add complexity, additional processing, and attack opportunities without first addressing weaknesses. –RAYTHEON CODEX

Complex and layered supply chains for software and firmware*:*

Third party software permeates everywhere, including in critical infrastructure, military platforms, and weapons systems. We cannot reason about third party software so we cannot reason about our systems and adversary systems. It also means we cannot reason about critical infrastructure.-Dr. D. Ghormley, Sandia National Labs

Software and firmware engineers often copy and paste code found on the Internet into their codebases. As a result, when reverse engineering a binary, it is common for the engineer to observe very similar 'binary blocks' even in software from different vendors- Battelle

Cyber speed conflicts*:*

This will fundamentally change when we are fighting a peer competitor (like China) where we both have AI. Now it is moving at digital speed instead of human speed, now it is not 1 target but 1,000 targets, and therefore, we are going to have to make deci-

a. **Increasing complexity and unnecessary code/features** in software, protocols, and system functionality, resulting in added cost, inefficiencies, and vulnerabilities.

b. **Increasing programmability in protocols, software, and even hardware**, leading to increased flexibility and speed of development. However, each new entity created by reprogramming is a potential source of new vulnerabilities, requiring new approaches to trustworthiness.

c. **Increasing roles of third party, open source, and other reusable software and hardware**, enabling rapid development and deployment of new products and services. However, this sourcing approach results in a large number of sources, layered supply chains, and possible loss of provenance information. In many cases, there is no access to the source code, thus forcing reliance on binaries for software analysis and verification, a major S&T challenge.

d. **Hyper-automation and shrinking timeline at all levels of cyber conflict.** Cyber speed conflicts require minimal, but strategic, use of expert humans. Thus, technologies that work autonomically to prevent compromises and/or minimize the mission impact after any compromise will be very valuable. Also valuable will be techniques and tools for increasing automation in 'cyber weapons factories'.

e. **Increasingly untrustworthy cyberspace environment** in which very little can be trusted. In particular, the location and ownership do not equate to trustworthiness. Assets, data, and information need to be protected against cyber-attacks based on their importance in mission context, irrespective of where they are located. These needs motivate the *Zero Trust Strategy and Architecture.*

f. **Increasing diversity among areas of applications of cyberspace** creating new cyber challenges and opportunities at the intersections of cyberspace and its application areas. All critical infrastructures, military platforms and weapons systems, and integrated cyber-physical-bio-neuro are examples of important areas of applications of cyberspace technologies.

g. **Increasingly tighter interconnections among cyberspace technologies** creating new cyber defense/offense challenges and opportunities where these technologies intersect. Tighter coupling between hardware and software due to major changes occurring in microelectronics architectures is one important example. This coupling will require joint verification, sensing, and actions for defense and offense. Interconnection between every ML technology and every cyberspace technology is another example of major interest. For example, ML processes and algorithms could face an adversarial cyber-attack that could corrupt training or test data, exfiltrate information about ML model, etc.

h. **Increasing scalability of Formal and Semi-Formal Methods and incorporation of useful cyber defense specifications** will enable wider use of formal approaches to specification, development, and verification of cyberspace technologies and systems.

i. **Increasing roles of cyberspace technologies in personal and professional lives, and military conflicts**. Increasing dependence on these technologies will create major vulnerabilities with perimeter-less impact. Adversaries will try to achieve asymmetric advantage to offset the US superiority in kinetic domain. Additionally, the blurred boundary between personal and professional lives will introduce new vulnerabilities to warfighters in theaters.

Trends in Individual Cyberspace Technologies and Their Applications

a. **Microelectronics**: 'Deaths' of Moore's Law and Dennard Scaling have motivated the industry to focus on innovative heterogeneous packaging. One example is the integration of multiple diverse smaller chips (Intellectual Property Blocks, Chiplets, etc.) in a single 2D, 2.5D or 3D chip. Combining heterogeneity within a chip with increasing use of Field Programmable Gate Arrays (FPGAs) will enable increased programmability and novel domain specific accelerators in hardware. These advances will continue to provide significant gain on the cost-performance curve. They will also blur the boundary between software and hardware, and introduce new vulnerabilities at lower architectural layers. On the other hand, they will enable new cyber defense mechanisms and instrumentation to explore.

> ***Microelectronics and packaging***
>
> *"Heterogeneous packaging is really the future. For the next several decades it is going to last. The race in heterogeneous packaging integration got started a couple of years ago. Every semiconductor company is scrambling to beat everybody else. That is going to create a mixture of domain specific architectures. 3D die stacking is going to be phenomenal in its potential for the future." – Dr. Aravind Dasu, Intel*

b. **Networking and communication for wireless access (e.g., 5G/6G, future tactical wireless for the DoD)**: Expected massive increase in device-device communication, heavy reliance on Software Defined Networking (SDN) and Network Function Virtualization (NFV), and a higher degree of programmability will allow rapid service development and customized cyber security. However, increasing centralization (via SDN) and speed of changes will introduce new vulnerabilities. Future DoD tactical edge networks may possibly be based on 5G/6G but could be different enough to bring additional challenges not addressed by the commercial vendors of standard 5G/6G products. Along with IoT, the enterprise versions of 5G/6G could revolutionize services for commercial/industrial campuses as well as military bases, all requiring high security and reliability.

c. **Networking backbone**: The Internet backbone could undergo one or both of the following significant changes: Balkanization (splintering); and a move towards Content Based Networking (CBN). The latter will introduce a fundamentally different approach to content storage and hence new data security challenges. The former will require innovative technologies for situation awareness and access. SDN and virtualization, if implemented broadly in the Internet backbone, will lead to the challenges and opportunities discussed in 'b' above.

d. **Core Computing**: Tensor Processing Units (TPUs), FPGA-based accelerators and custom chips (e.g., AI, Neuromorphic), custom processors, increased virtualization, and affordable heterogeneity will enable scalability of resource demanding algorithms, new computational approaches, and more sophisticated autonomic cyber defense. However, these trends add more software at lower layers, and a greater potential for vulnerabilities.

e. **Private- public-hybrid-, and multi- cloud computing** will enable almost any organization to have access to very high-end secure computing, otherwise available only to advanced nation states and large commercial entities. Virtualization, microsegmentation, and microservices will enable rapid creation of new services and highly customized security solutions. However, they will create dynamic and complex supply chains fraught with new vulnerabilities. Late-stage verification and automated corrections will be crucial.

f. Quantum timing, sensing, computing, and communication. Security of atomic clocks and standardization of Quantum Resistant Encryptions are near term challenges. Quantum sensors will pose challenges in mid- and far-term. Other capabilities created by quantum effects will have major impacts, but the time frame is uncertain.

g. Smart CPS, including autonomous mobile platforms. The universe of smart CPS is expanding due to increasing ‘cyberization’ (sensing, data movement, and data processing to improve system operations) of all critical infrastructures, vehicular platforms, and healthcare systems. The IoT and 5G provide lower cost sensing and rapid movement of data, thus accelerating this ‘cyberization’. CPSs provide strong mission context to cyberspace technologies and require a greater focus on the integrity and availability aspects of cyber defense. Increased ‘cyberization’ is also creating new challenges and opportunities at the intersection of cyber and physical aspects of CPS. Fusion of information from these two and coordinated actions in both provide more effective defensive and offensive technologies than independent observations and actions in cyber and physical.

> ***Cyber Physical Systems:***
>
> *$1.8T Weapons systems face two top challenges, SW and Cyber (GAO June 2020)*
>
> *Our reliance on computing to supervise, monitor, and control key pieces of critical infrastructure combined with the mass expansion of commodity computing create a massive attack surface. Our current attempts to defend these resources do not account for the sophistication of an adversary committed to damaging US interests- Raytheon CODEX*
>
> *Many existing techniques from software engineering can be inaccurate and error prone when applied to generic programs. But in the CPS domain, if we take a domain-specific approach and leverage the control model when applying these techniques to the control program, we can get more accurate results. Knowledge about the control model reduces the search space for techniques like fuzzing and debugging.-Professor. D. Xu, Purdue University*

h. IoT and Edge Computing add a large number of low SWaP-C devices to the network, enable high-density distributed sensing, and provide significant computational capacity closer to the data sources. However, low resource devices may be unable to support the best security solutions but will provide entry points to reach valuable targets in the network backbone. These challenges require a security solution based on the capabilities available in end systems as well as networks. A distributed trust model to generate trustworthy data from vulnerable set of IoT devices is another important need.

> ***Edge Computing and low SWaP IoT Devices:***
>
> *We are moving to edge computing, but edge may not be ready in terms of security. Constraint-aware cyber security and computation integrity will remain a challenge –Professor D. Xu, Purdue University*
>
> *IoT purpose does not include cyber, cyber is an afterthought with no memory and processing room left for it in-J. Li. Siege Technologies*

i. **Digital persona and deceptive content in multiple media** will enable innovations in authentication, while enabling novel deception techniques and creation of alternative realities

j. **Integration of bio, neuro, cyber, and physical:** Exoskeletons supporting humans, machines controlled by human brain via cyber speed interfaces, brain-computer hybrids working as a single entity, and brain to brain communication using brain waves will create a new world with very different models of human-machine teaming. This integration of inorganic (cyber and physical) and organic (bio and neuro) components will have a major impact on the cyber battleground.

k. **ML**: ML, including Deep Learning (DL), Reinforcement Learning (RL), and Deep Reinforcement Learning (DRL), has become the predominant source of techniques for Artificial Intelligence (AI), and will most likely continue in this role for the foreseeable future. ML will also continue to grow its multi-faceted relationships with cyberspace. It could assist almost all cyberspace technologies and their applications. On the other hand, advances in cyberspace technologies (e.g., TPUs, ML in chips, and Quantum Computing) will continue enhancing ML capabilities. ML could enable powerful new mechanisms for defensive and offensive cyber. However, cyber-attacks on ML processes and algorithms could neutralize these mechanisms or, even worse, make them work against the system being protected. Trustworthiness will thus be an important requirement for ML to be applied successfully .

1.3 Observations of Importance

Loss of Leadership in critical technologies

Microelectronics power all AI, and the United States no longer manufactures the world's most sophisticated chips. We do not want to overstate the precariousness of our position but given that the vast majority of cutting-edge chips are produced at a single plant separated by just 110 miles of water from our principal strategic competitor, we must reevaluate the meaning of supply chain resilience and security, - NSC AI Strategy.

In the future, when weapon systems need leading-edge IC to stay competitive against adversaries, DoD will likely need to rely on an unsecure supply chain in another country to meet those needs- IDA report on the vulnerabilities in supply chain.

China is pouring enormous resources into ML and has a long history of using cyberattacks for political and economic aims. ….. Unless the US makes an unprecedented and urgent investment in ML for cyber defense and attack, we will lose the race before it has hardly begun – Dr. H.Kautz, NSF

While not in the scope of the study, the team observed sentiments that are important to report here. These may require separate studies.

COTS vs GOTS vs Custom DoD technologies

The team noticed a sentiment from many experts that the DoD has become too dependent on COTS cyberspace technologies and has not even insisted on the customization needed for the DoD needs. Since the DoD requirements on security frequently conflicts with the commercial business models, there is potential for serious security risks. Additionally, the DoD essentially uses the technologies everyone else uses, with no differentiators. There was a feeling that the DoD should lead more and insist on strategic customization.

Loss of Leadership in Critical Technologies:

Another major concern was the loss of leadership in critical technology areas like microelectronics, 5G infrastructure products and critical chips, ML, ML hardware, and quantum. One result is an unreliable and untrustworthy supply chain for almost all critical hardware. Another possible impact is losing control of all our critical infrastructures. Finally, to many, it appears that we are losing intellectual leadership in several critical areas. There was a sentiment that the situation is bad and will grow worse in absence of significant increases to S&T investments in these areas.

1.4 Important Notes on the Study and Report

In this report, the descriptions of technology trends and required S&T are biased towards defensive cyber. It is important to note that the S&T efforts for both defensive and offensive cyber are important and, in many cases, the core technologies form the bases for both applications.

This study is not aimed at identifying gaps and recommending specific Cyber S&T investments. By discussing technology trends and their influences, the study brings to the surface high-priority future cyber challenges and opportunities that need to be addressed. Current plans may address many of these challenges and opportunities. The remaining should be discussed for future S&T decisions.

2 Study Background and Process

As mentioned briefly in Section 1, this study is aimed at identifying relevant technology trends, their impacts on the future cyber battleground and hence on the required S&T. The current section provides formal definitions of several key terms and details the process of information gathering, analysis, and summarization. Both of these will be useful in comprehending the rest of the report,

The term 'cyberspace' is used frequently so it is important to provide a formal interpretation. **Cyberspace is defined as a domain characterized by the use of electronics, electromagnetic spectrum, and software to store, modify, and exchange data via networked systems and associated physical infrastructure (2010-2011 Joint Terminology**

for Cyberspace Operations). This definition includes all microelectronics, computing, communication, and networking technologies and systems.

With that definition, our personal and professional lives, all critical infrastructures, and all Governmental operations are increasingly dependent on the cyberspace technologies. However, cyberspace is vulnerable to malicious attacks with potentially devastating consequences, serious enough that cyber defense has become a major industry and Cyber has become a warfighting domain with its own Combatant Command.

> *I think you're going to see every country in the world trying to develop an asymmetric capability that allows them to conduct espionage for cyber purposes and disruptive destructive attacks." – Adam Meyers, CrowdStrike*

The above definition also implies the Cyber S&T is not aimed at creating new cyberspace technologies. The goals of **Cyber S&T** are novel approaches and technologies to

- create desired effects on adversary cyberspace, and
- deny the adversary's ability to do the same to us

New cyberspace technologies developed and deployed by others will change the cyber battleground and influence the required Cyber S&T. The Technology Futures Study, sponsored by the DoD Cyber CoI, is aimed at developing an understanding of the trends in these influencer technologies and their impact on the S&T goals.

In view of the above discussion, the technologies of interest are categorized into three classes (no ranking implied):

- **Class A**: Technologies inserted in the cyberspace to provide major improvements in performance, capacity, cost and footprints, and to allow new applications of cyberspace. Examples are 5G, autonomous vehicles, IoT, ML, cloud computing, system on a chip, and brain computer interfaces
- **Class B**: Technologies that provide major improvement in computing speed and storage, thus allowing cyber defense and offense techniques not possible otherwise. Examples: GPU, TPU, multi-core, cloud computing, and quantum computing.
- **Class C**: Conceptual breakthroughs in techniques for cyber defense and offense. These could enable staying one step ahead of the adversary. Some examples are new approaches to automate the mitigation/weaponization of a vulnerability, reverse engineer binaries, or attribute different aspects of a cyber-attack.

Some technologies could belong to more than one class. A technology trend may include multiple technologies working together. In addition, new approaches and business models used to develop and deploy cyberspace products and services may create major new cyber challenges and opportunities. The study includes these non-traditional trends along with the trends in specific technologies. Greater focus is on Class A and Class B as they provide truly external influences. Class C technologies play two roles in the study. On one hand, the study identifies the goals of future Cyber S&T in the form of expected new Class C technologies. These are discussed as S&T goals rather than influencers. On the other hand, the past and recent S&T efforts have generated technologies that have partially met some of the S&T goals and promise to provide jump starts for more. Such technologies could be both influencers and goals. In this study, those are mainly discussed as part of the S&T goals but with some indication of the current status of accomplishments. The following are some examples of such technologies:

- Software program analysis
- Binary reverse engineering
- Formal Methods for cyber properties
- ML, especially, DNN, DRL, GML, and GAN
- Autonomous agents
- Chips with ML capabilities
- Pattern analysis in encrypted data

Note that the above, while providing jump starts, need ongoing S&T themselves to enable advances in cyber defense and offense.

Multiple types of sources were used to collect information about the technology trends.

- External Sources
    - 16 Request for Information (RFI) responses by industry
    - 20 survey responses from FFRDCs, UARCs, and researchers in industry, academia, and Government
    - 45 interviews with experts in academia, US Government Labs, FFRDCs, UARCs, defense contractors, and commercial industry. Each interview lasted approximately an hour and resulted in up to a 10-page report.
    - Roadmaps from other DoD Reliance 21 CoIs and Principal Directors (PDs) for the DoD Modernization Priorities
    - Approximately 80 documents:
        - Long range planning documents, strategy documents, futurist reports, and other relevant material from US Government organizations.
        - External presentations and studies on relevant future technologies
    - Published technical papers
- Expertise of the team members and their colleagues.

The above mix of sources provided a very broad coverage as well as depth. The inputs were categorized by major technology areas. The study team summarized findings for each of these major areas. These summaries, totaling over 300 pages, provided the basis for this report. It should be noted that the views expressed in this report are distilled by the team members based on the inputs from all the sources listed above, including the expertise within the team. There is no attempt to reflect all viewpoints on any particular topic.

The rest of the report is organized as follows. Section 3 provides details on major technology trends, their impacts on the cyber battleground, and the resulting Cyber S&T goals. While the focus of the study is on the technology trends, some other trends with potential for major influences on the cyber battleground are discussed briefly in Section 4. Some technologies could have dramatic impacts on the cyber battleground but there are major uncertainties in the likelihood and timing of their realization. These are discussed briefly in Section 5 as futuristic projections. Section 6 provides a summary of findings and recommendations. Some observations and insight deserving of further investigations are presented in Section 7.

3 Key Technology Trends, Impact on Cyber, and Cyber S&T Goals

This section provides more detail on the technology trends, their impact on cyber battleground, and the Cyber S&T goals motivated by the predicted impact.

3.1 Increasing Complexity and Road to Minimalism

Systems of systems using cyberspace technologies are getting increasingly complex and difficult to understand, characterize, control, and manage. The complexity could create an environment where emergent rather than designed behavior drives the control and management. Some complexity is the natural result of an increasing reach of the cyberspace, uncertainty in novel tasks, and interconnected nature of the systems being supported. However, the ways in which cyberspace technologies are developed and deployed in systems add to the complexity and difficulty in control and management. These processes could also add unnecessary features in system architecture and protocols, and code that is never used. This unnecessary baggage (bloat) results in inefficiencies and cyber vulnerabilities within cyberspace technologies as well as their applications. Some examples of contributors to complexity and bloat are discussed below:

1. Since the cost of human developers is increasing while computing and memory are getting cheaper, it is easy to build software libraries and modules and insert them in integrated systems. The ubiquity and standard practice of leveraging third parties and open source create the distinct potential that a significant portion of the resulting software may never be used, and an even larger fraction may not be used for a given mission deployment.

Additionally, without strict code reviews and significant testing, the chance that the code paths will perform as intended or desired in a specific use case is questionable.

2. Every protocol is designed to provide services to the higher layer and typically supports the union of all features needed by all applications. For a given deployment environment, only a fraction may be needed. This is also true of software layers. Union of all things needed by all applications is thus a minimal requirement for the design but only a fraction is needed for one environment.
3. Backward compatibility is a strong requirement. Since most new protocols and software versions are required to work with older versions, they may carry additional features and code and thereby carry-forward inefficiencies and vulnerabilities from these historical versions.
4. Practice of grandfathering everything that is present in the systems deployed now but may not be required anymore for the proper functionality.
5. Legacy systems where new features and codes are added without a redesign and testing to see what parts of the original system are still needed
6. Software-as-a-Service offerings can be transparently updated without user awareness. Applications increasingly instrument the device they run on in order to aid troubleshooting and future optimizations (i.e., Customer Experience Improvement). Complexity and bloats are added without the knowledge of the user.

Deciding which features and which parts of code can be removed without impacting the ability to deliver services needed by the mission is not easy, making it difficult to simplify and debloat. Complexity adds to the difficulty in identifying removable code and features. Bloat makes the system inefficient and more vulnerable to cyber-attacks. When the cost of the system is based on metrics like lines of code, the bloat also adds to the system cost. Experience has shown that 50-80% of code in typical software systems could be complete bloat (never used) and even a larger fraction may not be needed for a specific application.

The above discussion suggests the following S&T efforts.

a. Identification of the 'maximum set' of removable features and code for legacy systems. This set could be used to debloat before deploying. If possible, the debloating could be performed for each mission by late-stage customization. Also, for legacy software, it is important to develop technologies to perform debloating and customization on binaries. Effectively taking what is needed but little more.
b. A new approach for developing minimalist but easily expandable future systems. In particular, the goal is to design and develop small modules that can serve as building blocks and provide a repository from which a system developer can choose and integrate into a system, ideally for each mission. This approach could lead to simplicity, efficiency, and security.
c. Maintaining the above minimalist philosophy as the abilities to automatically design and develop protocols, software, and hardware materialize. Automation and minimalism frequently conflict so this is a serious S&T challenge.

3.2 Towards Programmable Everything

Until recently, most of the core hardware, software, and network infrastructure came hard-wired from vendors and integrated to create systems and networks offering services to the users. There is a clear trend towards increasing programmability in all cyberspace technologies and their applications, starting with higher layer application software down to devices and chips. Programmability allows the same lower-layer infrastructure to be used for multiple customized services to higher layers via middleware and APIs. It facilitates faster time to market and cost-efficient offering of lower volume services to higher layers. Programmability does impact the performance and efficiency and may make higher volume services more expensive compared to the same services offered by the hard-wired counterpart. In general, the 'users' of a programmable lower layer gets more control of services they receive or provide to higher layers. This control also generates new cyber-attack vectors at the interface. In many cases, the programming of services at an interface may involve third party products, adding more attack vectors. On the other hand, the control may also offer opportunity to add sensors and analytics to monitor the interface and provide resilience against vulnerabilities at the lower layer. Both pose new challenges and opportunities for Cyber S&T on defensive as well as offensive sides. The actual challenges and opportunities may depend on which layers are involved, what is programmable, and how the programming is done. Since end-to-end cyber defense now depends on programming at multiple layers, by multiple entities, at different stages in the development, another S&T challenge is to identify the right mix of formal methods, vulnerability analysis and mitigation, and resilient design for each layer.

Some likely and important programmability trends are discussed below:

3.2.1 Application Software and Network User Services

These have been programmable for some time now. Open source, third party, and/or the end user could program and control these.

3.2.2 Programmable Networks

3.2.2.1 Software Defined Network (SDN) and Network Function Virtualization (NFV)

SDN and NFV are discussed in more detail in Section 3.10. In short, SDN allows centralized control and management of a network domain, more or less independently of the underlying network infrastructure technologies. NFV allows the use of commodity hardware to execute any networking function and locate it almost anywhere in the network. The net effect is easy programmability and rapid creation of new services.

3.2.2.2 Programmable Network Devices and S&T Goals

An artifact of SDN, NFV, and low-cost merchant silicon devices is increasing programmability in switches and routers. In addition, many vendors have adopted mainstream Linux components such as Containers. So, it is now possible to execute a variety of codes on an embedded network device with very close access to the data plane. The following S&T goals are motivated by increasing programmability in network devices.

a. Technologies for distributed cyber defense facilitated by increased programmability of network devices
b. Increased level of sophistication of deep packet inspection algorithms for detecting cyber-attacks, taking advantage of local processing to mitigate the need to transmit large, collected flows
c. Defense against new vulnerabilities from NFV in network devices. For example, running microservices on Linux Containers in network devices introduces the possibility of significant vulnerabilities and a large attack surface. If able to break out of the container, denial of service attacks and privileged access to network data are possible.

From Programmable to Intelligent Networks and S&T Goals

- Current programmable and virtual networks enable many new applications. However, they are complex, immature, and could have major security holes even after 10 years in the field.
- The next stage could be “smart networks”: Networks that can take care of themselves, and react faster than the humans; reduction in security holes over time; and increased usability, enabling more applications.
- Smart networks will be followed by “autonomic/autonomous networks”, the difference here being that human need not be in the loop. Like self-driving cars, these networks will move and function on their own.
- As discussed in Section 3.10, 5G already offers tremendously more programmability than 4G in terms of offered Quality of Service (QoS), access controls, edge vs cloud computing optimization, etc. 6G is supposed to go close to truly autonomous networks with ML techniques built into protocols and controls. However, taking human out of the loop will require reliable resistance and autonomic/autonomous resilience to cyber-attacks. Significant S&T effort will have to be devoted to ensuring these.

Thus, the following S&T effort is important.

d. Ensuring that the techniques developed for prevention of compromise and autonomic resilience are moving towards automation, and the algorithms and data remain trustworthy without HIL

3.2.2.3 Programmable Hardware, Processors, and Computers, and Related S&T Goals

As the programmability extends to hardware, processors, and computers, new challenges and opportunities emerge, thus leading to new S&T goals.

a. Rapid verification of each customized version of a processor. The proverbial pendulum is swinging from general purpose processors to special purpose programmable hardware. In theory, such programmability and customization could allow the required functionalities to be implemented with unnecessary features and code, thus offering management and security advantages. On the other hand, significant effort will be needed to verify each customized version for correctness and security.
b. Trustworthiness and cyber defense applications of in-situ self-modification of FPGA based on learning from experience. At the hardware level, FPGAs already offers programmability. However, FPGA configurations are typically planned in advance or sent as a manual firmware upgrade to a system. It is technologically feasible to design such a system to modify itself based on the functions it is asked to perform, data it encounters over time, and attacks/faults it experiences. Research is needed to determine the degree to which this self-modification capability could be achieved based on intelligent in-situ learning and decision making, its potential use for cyber defense, and new vulnerabilities resulting from its use.
c. Defense against new attack vectors (including new side channel attacks) resulting from added FPGA programmability. Use of the added programmability to insert self-monitoring capability. Microsoft has made a new paradigm more popular for FPGAs. Effectively, an FPGA is programmed to make it act like multiple FPGAs, each with additional programmability. C++ compiler could then talk to System on Chip (SoC) and ISA core. Architecture and instruction set can then be changed every month or so, offering a lot more programmability and customizability. However, cybersecurity could take on a very different profile with this level of programmability. Open source and third-party software could now access FPGAs. There could be new side channel attacks. Vulnerability assessment, mitigation, and verification need to happen close to deployment time.
d. Supply chain controls and verification of heterogeneous chips with programmable components. These tools should be (semi)-automated, and data driven and may need some explainable ML in the toolbox.

   Programmability is going down even lower to the hardware level. As discussed in Section 3.9, smaller components (including chiplets) from many vendors could be brought together and integrated by the packaging houses. FPGAs could coexist with ASICs to make the whole chip programmable. This is a fundamental change in hardware architecture. It is important to develop a rich set of tools to help win the resulting cat and mouse game.

3.3 Third Party Everything and Evolution to Open Ecosystems

3.3.1 Software

Software has become the critical building material for the entire cyberspace and its management. Even important new techniques in autonomy and machine learning are realized by software. Design and production of software systems have become complex and expensive, and developers/coders have become very specialized. Thus, a complex integrated software system could use modules from a variety of sources: third parties; open-source libraries; and controlled code libraries. Third party software itself could use modules from open source or controlled code libraries. A software stack made up of layers of software could have modules from one or more sources at each layer. Programmability of software layers make it even easier to use this Lego approach to building complex software systems. Updates to the software modules could also come from third parties. In some cases, third party software may even be used as a service while executing user workload. The software supply chain is becoming multi-layered and complex. DevOps formalizes this approach.

It is not easy to reason about third party software and hence about friendly and adversary systems, including critical infrastructures, military platforms, and weapons systems. It is also difficult to fully adjudicate and verify such software. Complex, multi-layer supply chain makes it even harder since the source of the software may not be easily visible and the software can be tampered with at many stages. It is not clear what was verified when and by whom. In many cases, source code may not even be available.

These difficulties point to the need for the following S&T.

Where source code is accessible and analyzable, methods and tools for **late stage**

a. formal verification of implemented code
b. fuzzing, concolic analysis, verification, and other tools for vulnerability discovery
c. vulnerability exploitability analysis and mitigation, possibly using ML

Given that dynamic code libraries are significant sources of modules in modern software systems, it is important to develop techniques to ensure that the modules in these libraries are verified before being made available.

d. Configuration control of dynamic code libraries. Each linked module could possess a unique identifier (hash) to a known good instance and any updates or changes could be validated against the functionality of the known good instance.

For binaries, methods and tools for **late stage**

e. reverse engineering, static and dynamic analysis, and structure recovery
f. verification and vulnerability discovery
g. exploitability analysis of vulnerabilities and mitigation
h. binary transformations, binary diversity, and binary debloating (for minimalism and resilience)

This late-stage analytics on binaries would allow identification of vulnerabilities in binaries, find mitigation, and formally verify the resulting new binary.

The importance of late stage analysis and verification implies the need for speed and automation.

3.3.2 Firmware and Hardware

Third-party software could be used for customizing FPGAs and third party HW components (including chiplets) could be used to assemble a new System- on-Chip (SoC) quickly. Both add tremendous flexibility and speed in introducing new capabilities in chips. However, they add multiple new attack vectors through the complex supply chain, thus resulting in the following S&T goals.

a. Control of complex supply chains with significant third party components (including chiplets)
b. Late stage, rapid verification of heterogeneous chip
c. Late stage, rapid verification of third-party code used for customizing FPGA

3.4 Hyper-Automation: Shrinking Timeline and OODA Loops at Multiple Time Frames

Immense increase in connectivity and computing capabilities, coupled with sophisticated data collection techniques using social media, shopping and traveling behaviors, and sophisticated sensors, are generating massive amount of data about individuals, society, infrastructure, commerce, and Government. Increasing sophistication of data analytics techniques, coupled with increase in computing power, has enabled the resulting machine intelligence to provide stronger decision support in almost every decision human has to make. As the confidence in machine recommended decisions increase, human decision makers rely more on those recommendations and intervene only where they feel the need to control. Thus, there is a trend from all human decision making, to machine assisted human decision making, to human assisted machine decision making, to all machine decision making with human on the loop (HOL) rather than human in the loop (HIL). Of course, the progression occurs at different rates for different decision types. The overall impact is shrinking timeline and radically shortened OODA loops for many decisions in personal and business lives, system controls, and military conflicts. Speed as well as quality of decisions become important and winning the time race becomes a key determinant of success. The following are implications for cyber warfare.

3.4.1 Importance of Preventing Compromise

One important aspect of prevention involves reduction in the density of cyber vulnerabilities before the system deployment to minimize the probability of a compromise and hence the need for human involvement during the operational phase. It also involves continuous identification and mitigation of cyber vulnerabilities after deployment but before an adversary can exploit them, and thus winning this portion of defense-attack timeline battle. Finally, prevention also involves automated access controls to minimize the presence of unauthorized users in the system. The following are some examples of technologies that may help achieve these goals:

a. Automation of the process starting with vulnerability discovery to mitigation and verification of
   I. architecture and design
   II. protocols
   III. software source code
   IV. binaries
   V. hardware, and firmware

These goals and related S&T are critical for identifying and mitigating vulnerabilities before an adversary finds and weaponizes them. As discussed for all goals involving automation, the progression here could start with machine intelligence and tools assisting humans and move to humans assisting tools, and finally to full autonomy without HIL. The progression could be at different rates for software, hardware, protocols, and architecture. Automation of vulnerability discovery in software is the farthest along. Techniques like fuzzing, static and dynamic program analysis, symbolic and concolic execution, have enabled a set of tools to assist humans and are moving to go towards the next step of human assisted tools. Also, automated patching and software repair are already in the realm of possibilities. Assistance from DL techniques could help improve scalability and speed. Automation of vulnerability discovery and mitigation for protocols is at the beginning stage. Sometimes, specifications in text and diagrams form need to be converted to machine understandable specifications that can be used to search for vulnerability, and that, itself, is an S&T challenge. During the progression from tool assisted human decision making to removal of human-in-the-loop, the technologies that facilitate optimal human-machine teaming will play a major role in the success of cyber defense and offense. ML could provide useful methods and tools to achieve these S&T goals.

b. Formal guarantees via the use of formal and semi-formal methods for **specification and verification** of the cyber defense capabilities of architecture, protocols, software, hardware and firmware. These could be applied to new systems as well as implemented systems. Section 3.7 discusses specific goals for S&T in Formal Methods.
c. Formal and semi-formal methods for **automated design, development, and** verification from specifications that include cybersecurity. In particular, automated development of provably secure software from specifications.
d. Encryption and multi-factor authentication for devices. Fully automated access control using Public Key Infrastructure (PKI) based authentication and authorization is already in use. It is important to ensure that those remain effective as more devices (non-person-entities) are added to the networks. For examples, can we trust the protection of 'what you have' portion of multi-factor authentication? Can more sophisticated encryptions of the future be implemented in these devices?
e. Space and time diversity in software, firmware, hardware, and protocols performing the same functions. The goal is to increase the work factor for an adversary to compromise the systems by changing between reconnaissance and attack. That is, providing SDD and MTD. Section 3.5 provides more detail.

There has been S&T effort and useful results for some of the above, but much remain to be done, especially for a-c.

3.4.2 Post-Compromise Minimization of the Impact on the Missions without using Human-in-the-Loop (HIL)

Since compromise can never be prevented with certainty, the next lines of automated defense are techniques that act, without HIL, to minimize the impact on the mission even if the system is compromised. Several types of mechanisms could be used:

a. Autonomic triage and resource reallocation to minimize the impact on the mission critical functions. This approach is used in networking and computing in general to ensure that limited resources available after any failure or attack are used for the most mission critical functions. The additional challenge in cyber is to ensure that the mechanism accounts for correlated impact of an attack.
b. Isolation to protect against the spread of a compromise. Important to capture the mission context to prevent one-size-fits-all response that could be detrimental.
c. Spatial diversity to limit the number of devices that can be compromised with one exploit (SDD). This takes advantage of many computing and communication functions that can be carried out by different variants in different devices. Innovations are in creating variants that provide same functions but cannot be compromised using one exploit.
d. Time diversity to eliminate or minimize the time an adversary could exploit the compromise (MTD). The diversity is similar to that in 'c' above, but the variant to be used are changed dynamically. MTD could also act in presence of SDD by moving around the variants used by different devices, that is dynamically changing the device to variant mapping.
e. Deception and other cyber maneuvers. Innovations are in both developing deceptions and tailoring based on attacker and attacker moves.
f. Innovative sensors, analytics, and autonomic rapid recovery
g. Mission and context aware autonomic responses, especially for cyber physical systems where the trade-offs among confidentiality, integrity, availability, and control are different and better understood compared to those in general purpose computing systems.
h. Use of autonomous agents with ML capabilities. This is another promising technique for resilience. The orchestration of capabilities provided for 'a', 'b', 'e', and 'f' are promising areas for autonomous agents. Developing ML techniques that can be used in real time and are robust against countermeasures (adversarial ML) are important S&T goals. More detail on the need for Trustworthy ML is provided in Section 3.17.4.
i. Autonomic resilience mechanisms for increasingly more untrustworthy environments. This goal will be discussed in more detail in the context of Zero Trust strategy. Two specific mechanisms of interest:
    i. Layered encryption and self-protection of data objects depending on the importance to the mission.
    ii. Authentication and authorization of users as well as services interior to the system. Time-limited or per session authorization.

There has been significant research effort on several of the above, especially for a-e. Technologies for 'a' and 'b' are quite mature, but the challenge is in representing the mission context appropriately so that the responses are context aware. More detail on 'c' and 'd' can be found in Section 3.5. SDD and MTD techniques discussed there need further S&T to down select the effective techniques, develop guards against many side-channel attacks (especially those from speculative execution), develop robust orchestration, and ensure that the techniques are natural part of the workflow. Much work has also been done for item 'e' above, but late-stage customization capability is needed to get more value out of the results so far. Item 'g' is very promising and discussed further as part of the CPS in Section 3.13. Items in 'i' are important S&T topics and play major roles in Zero Trust strategy. They are discussed further in Section 3.5.

3.4.3 Rapid and Cost-Effective Generation of Effective Cyber Effects and Access. Responsive and Cost-Effective Cyber Weapons Factory

To some extent, these S&T goals are offensive cyber counterparts of the automation goals in defensive cyber S&T, with some key differences in the importance of predictability and controllability.

a. Automation of process from vulnerability discovery to development and characterization of effects and access. Vulnerabilities could be in the system architecture, protocols, software, hardware, and firmware. As for the defensive cyber, there will be a progression with increasing autonomy. ML techniques could help.
b. Extending the above process to binaries
c. Automated prediction of the consequences of the use of a cyber-weapon
d. Technologies for automatically mapping a small number of vulnerabilities to many more cyber-weapons with signature diversity
e. NLP to automatically translate descriptions of architecture and protocols from text and diagrams to machine understandable specifications
f. Use of ML in the process of automatically generating access and effects. The controllability and predictability play even bigger roles here. Else, we may have situations similar to the escape of a bioweapon from the lab.
g. Automated network discovery tools that work in resource constrained environment

Within ML techniques, genetic algorithms, DL, GML, and GAN seem promising, especially for 'a'-'e' above.

3.4.4 Automation in Cyber Maneuver after an Adversary System is Compromised

Automation in post-compromise offensive cyber maneuvers is the cyber offense counterpart of cyber resilience without HIL. However, the fact that the cyber weapons are in adversary systems change the required technologies and hence the S&T goals.

a. Automated sensing, local analytics, and well-defined actions like lateral movement and privilege escalation
b. Automated stealth, evasion, and morphing
c. In-situ customization and targeting by the cyber weapons
d. Automated repurposing of adversary malware to attack the attacker
e. Software agents that carry out cyber maneuvers based on sensor observations and the defensive response from the adversary. Together with software agents used by the adversaries, these could lead to cyber defense-attack moves and countermoves by software agents.

3.4.5 Tools to assist human actors with Cyber SA and Cyber C2.

While Sections 3.4.1 through 3.4.4 discuss technologies to manage cyber defense and offense with minimal, if any, involvement of humans during system operations, full automation without any HIL is unlikely in foreseeable future. Meanwhile, it is important to make human based cyber operations more responsive and be as close to cyber speed as possible. Two broad categories of capabilities required are Cyber Situation Awareness (Cyber SA) and Cyber Command and Control (Cyber C2). The former involves collection and analysis of the data on the cyber-state of the system and present the results to the decision maker as SA. The latter involves the use of the SA to assess mission impact and evaluate responses for their effectiveness. Both are becoming more complex with advances in cyberspace technologies and growing domains of their applications. Amount of data available for Cyber SA is increasing at a rapid pace and control actions are spread across increasing number of devices. Major reduction in analysis and decision time needs to be accomplished in the face of the increasing complexities. Of course, increasing computing speeds in processors of all sizes and increasing networking speeds allow distributed analytics and controls, which can be used to accomplish the required scale and speed.

Automation in building Cyber SA could include rapid analytics for the following.

a. (Obfuscated)-signature and anomaly detection

b. Adversary characterization and attribution
c. Malware analysis and attribution
d. Tracking adversary movement in cyberspace
e. Battle Damage Assessment (BDA)

Automation in Cyber C2 could include the following areas.

f. Assessment of mission impact
g. Evaluating cyber maneuvers such as deception, evasion, stealth, and morphing. Assessing likely consequences of various actions, and finding the best action
h. Simulation/emulation and digital twins

All of the above could benefit from ML techniques as discussed further in Section 3.17.3.

3.5 Cyber Redundancy, Heterogeneity, Diversity, and Dynamics

Redundancy is needed in almost every system performing critical functions. The purpose is to allow some degree of service to mission critical functions between a failure and the completion of repair. Of course, the system should be designed to minimize the probability of simultaneous failures of all resources that could provide the same function. In addition to the physical redundancy, cyber requires cyber diversity so the same attack does not compromise primary and backup resources together. Also, for cyber, heterogeneity and diversity play roles beyond continuity of operation. Maintaining confidentiality and integrity of data, in addition to availability of systems, after a compromise thus becomes important. And, in some cases, this can be accomplished without HIL, thus providing autonomic cyber resilience.

Cyberspace homogeneity has been a great productivity agent and cyber defense nightmare for the cyberspace infrastructure and services. Homogeneity of cyberspace infrastructure allows new capabilities to be deployed rapidly and cost effectively, makes interoperability easier, and makes management relatively simple. However, a single vulnerability can be exploited to compromise thousands and even millions of devices because all have the same protocols, stacks, and software.

Fortunately, technological advances over the last 15 years or so has made it possible to create variants (dialects) that could provide the same function with enough cyber diversity that the same cyber-attack could not compromise all variants. Such capabilities exist for software source code and binaries, firmware, computing stacks, memory addressing, and IP addressing. There are tens of ‘things’ that can have such variants and many of them can now be implemented inexpensively with affordable processing and memory overhead.

It is possible to change the variant from one system to another, from one Container to another, and from one time period to another. They can also be changed based on triggers.

The spatial diversity defense (SDD), where the variant (dialect) changes from one place to another, prevents an attacker from using one exploit to compromise many systems, many devices in a system and many Containers in the same hardware.

Time diversity (dynamics) provides a moving target to the attacker and hence is called ‘moving Target Defense’. (MTD) serves two purposes:

- Prevention of compromise: The system changes from the time of surveillance to time of attack to prevent a compromise
- Resilience: The system changes even after a successful compromise and limits the time the attacker can exploit the compromise (collection and exfiltration, escalation of privilege, lateral movement, etc.). The space and time diversity could be combined to move the Container-variant (or device-variant) mapping and where a given workload is executed.

MTD has been highlighted in 2009 and 2011 as critical component of cyber defense research and a memo from DEPSECDEF in 2018 mandated use of MTD techniques in new weapon systems. Given the visibility, MTD is sometimes used for discussing SDD also. The flurry of research activities resulted in many possible moving targets. However, different MTDs have extreme differences in utility and a combination may have to be orchestrated based on the system and threats. Also, SDD could have a very different effectiveness compared to MTD.

On one hand, MTD and SDD provide critical techniques to increase the workload for the attacker and change the attack-defense work balance. On the other hand, they could increase management complexity and lead to other attacks that could jeopardize system availability. Also, many side channel attacks could leak enough information to neutralize MTD (SDD less so). In particular, speculative execution creates side channels that could significantly jeopardize the effectiveness of MTD.

Success of SDD and MTD will depend on identifying the right set of entities to be used for spatial and time diversity and developing right orchestration that fit well into the workflow. They need to work in real environment with little human involvement.

As mentioned earlier many entities have been identified for MTD and SDD. The following four are relatively new and promising.

- Binary diversity in legacy systems
- Protocol diversity (dialects)
- Instruction Set Architecture (ISA) diversity. As cyber exploits are generally ISA specific, the use of dynamic heterogeneous computing can fundamentally break the exploits. Hardware-enabled MTD and SDD could be more robust.
- Microarchitecture level diversity.

In addition to the MTD and SDD discussed above, a very effective technique involves regular backups and periodic restart.

The above discussion motivates the following S&T goals.

a. Evaluation of the effectiveness of various entities to be used for SDD and MTD and identification of the most effective subsets acting together
b. Analysis of the impact of side channels and techniques to mitigate them
c. Design of the workflows and automation to make SD and MTD effective and easily manageable.
d. Design of effective microarchitecture level variants

3.6 Increasingly Untrustworthy Cyberspace: Zero Trust Strategy (ZTS+) and Architecture (ZTA+)

Note: In what follows, Zero Trust Strategy (ZTS) has been given a broader interpretation than its original, narrower, scope. That scope focused on going beyond the perimeter access controls and restricting access to any specific data object to human and non-human users based on the access control policies that account for their roles and needs for the data object in the mission context. The trends in the ecosystem of cyberspace technologies and applications require a broader interpretation for the future. Recent wave of very consequential cyber-attacks underscore the need for such a broader interpretation. The use of + in ZTS+ and ZTA+ emphasize the broader interpretation.

Enterprise computing and networking trends include remote users, bring your own devices (BYOD), and cloud-based assets. In addition, the uses of third party software and hardware, open-source software, and dynamically acquired microservices are increasing. Together, these trends imply that little can be trusted based on the location and ownership of physical assets, software, and services. Merging of personal and professional lives via social media and massive data breaches make it even harder to use simple perimeter based cyber defense. A new approach is required. Hence came the Zero Trust Strategy (ZTS+).

Zero Trust is a strategy not a product. ZTS+ and associated computing and communications architectures facilitate control, confidentiality, integrity, and availability of data and systems in increasingly untrustworthy eco-system and perimeter-less computing environment. The strategy assumes that little can be trusted inherently and that the architectures, designs, protocols, and operational policies should manage mission assurance despite untrustworthy people and systems in our midst. While many cyber defense mechanisms used today provide some Zero Trust capabilities, Zero Trust concept represents is a basic shift in the mindset for defensive cyber. All users and assets are assumed to be potential sources of vulnerabilities and data is to be protected based on its importance. Authorizing (not just authenticating) users and devices based on dynamic data access policy are now critical functions of cyber defense, irrespective of who and where the user is and where the data and assets are located. One important implication is the new need for strong security solutions for internal network and assets.

While ZTS+ is a strategy and architectural guidelines, there has been effort to add some detail into important requirement and characteristics of the solutions.

- Single strong source of user identity
- Time-limited authentication of human users and machine users
- Additional context, such as policy compliance and device health
- Authorization policies to access individual applications and data objects
- Access control policies within an application and between applications
- Service specific access controls
- Continuous monitoring of assets, users, and communication. Monitoring packet content, including within tunnels
- App-centric, built-in, cross-platform security controls. Ideally implemented in hypervisors for scalability, streamlining, and performance

The following are some S&T Goals motivated by the above:

a. Internal authentication and authorization between applications, between systems, and between vendor and user systems. Inter-service, application centric controls
b. Layered encryption for data objects with real time authorization based on the requester and roles.
c. Self-monitoring and protecting data objects
d. Cryptographic computing: Complete and Partial Homomorphic Encryption (HE); Secure Multi-Party Computation (SMPC); Privacy Preserving Search (PPS).
e. Further attention to monitoring packet contents, not just headers. Monitoring packets inside every tunnel to prevent adversary from riding the tunnel back.
f. Verification of every software and updates loaded into the system, irrespective of the source
g. Discovery and mitigation of cyber vulnerabilities introduced by new access controls and authorization, and new inter-services firewalls

DoD strategic networks and systems are similar to their commercial counterparts with some key differences in cyber risk tolerance that should be accounted for in developing/customizing solutions. However, the DoD tactical networks are significantly different. Zero Trust architecture and designs in this context require a thorough understanding of the implications of current architectures when people and devices cannot be trusted irrespective of where they are located and how they are connected. This will help decide the desired characteristics in Zero Trust tactical networks and system.

h. Evaluation of the security profile and trustworthiness of the DoD tactical networks in view of the increasingly untrustworthy eco system

3.7 Formal Methods

Formal and semi-formal methods use mathematical or logical formalism in specification, development, and verification of systems. A formally verified system is ‘guaranteed’ to meet the formal specifications.

Formal Methods have seen major research attention over the last four decades, as demonstrated by the plethora of papers and conferences. Tools have been developed to assist humans in specification, development, and verification. Industries have used and continue to use formal and semi-formal methods for critical physical systems. For over two decades, the FAA and NASA have been using increasingly formal approaches for approving systems for use. Companies like Boeing and Amazon have started using formal methods for physical and cyberspace systems. Most of applications of formal and semi-formal methods have focused on correctness and reliability, and the overall use is much less than expected from the attention by the research community. Their use for cyber defense and offense in adversarial settings is still relatively sparse.

Generally, formal methods suffer from scalability challenges, making the approach difficult for complex and heavily interconnected system of systems. In addition, their use for systems involving significant cyberspace technologies pose new challenges in specification, development, and verification. In particular, desired properties of software are difficult to specify. Further difficulties are added by the complexities and dependencies due to interconnections of hardware, software, and a wide variety of application domains, including enterprise computing and communication, electrical grid, military platforms, and weapons systems. When formal methods are to be used for cyber defense and offense, the specifications and verifications need to involve negative properties in the face of cyber-attacks, a difficult task. The increasing use of ML in cyberspace as well as application domain systems adds another layer of complexity for formal methods.

Currently, the use of formal methods involving cyber defense of complex systems is limited and fully formal approaches are not scalable even to moderate-sized systems. However, promising early results have been obtained in several dimensions, suggesting that further S&T along those lines could extend their suitability for more complex systems. Promising S&T directions are discussed below.

a. Useful specifications. Meaningful specifications leading to ‘fit for use’. Note that a formal verification only guarantees properties defined formally in the specifications. It is therefore important to ensure that the specifications, when verified, provide meaningful guarantees in mission context. Thus, the following questions should be addressed in developing formal specifications: What is the value of knowing that a software system is formally verified? Is that software ‘fit to use’ in a mission context? Does it have an acceptable risk profile? How can ‘fit to use’ properties be translated to formal specifications that are verifiable? The FAA has developed a set of ‘overarching properties’ for aviation systems that they use to approve/deny requests for inserting new technologies. The request is approved if and only if all properties are present. What are such ‘overarching properties’ for software in a mission context? What are such properties for broader cyberspace technologies?

b. Specifications and verifications for already implemented systems, especially protocols and software. Another promising Cyber S&T direction is the use of formal approaches for systems already implemented. That is, formal specification of the desired security properties for existing systems and formal verification of these properties. The techniques developed for formal verification should not just provide a binary ‘success’ or ‘failure’ result, as done by many verification techniques. Instead, they should identify where and why the verification failed and help identify mitigation. With these more ambitious goals, the S&T in this area could provide valuable tools for vulnerability discovery, mitigation, and verification for implemented systems. This approach has been used to discover flaws in an implemented protocol and verify the corrected version.

c. Building block approach. Given the scalability issues with formal (and even semi-formal) methods, it is productive to start by applying formal approaches to key manageable sub-systems and then using formal composability methods to extend the approach to progressively larger sub-systems, to entire embedded systems, to large platforms and weapons systems, to general computing systems and networks. An example is the formal verification of the correctness and security properties of the L4 microkernel as part of the DARPA’s High Assurance Cyber Military Systems (HACM) program. It took about 100 expert-years to achieve this. A Government-Academia-Industry consortium and a center of excellence are working to develop tools to speed up and scale the verification. One S&T direction is to move up from microkernel to the entire software stack for small embedded systems. From there, the applicability could scale up further.

d. Hardware for Root-of-Trust role. Building systems around formally verified hardware, which acts as a root-of-trust for higher level component and systems, including edge computing devices and CPS.

e. Simultaneous Specification and Verification of multiple layers, including software and hardware. Trends in microelectronics suggest that the hardware-software boundary is getting fuzzier and the contract between them via ISA is breaking. As a result of this tighter coupling, it will become important to specify and verify hardware and software together, especially, the interface layer. Joint specification and verification will have to deal with different semantics and state space multiplication.

f. Formal methods to specify and verify properties at the interaction of cyber and ML. Formal methods for ML is an important S&T topic by itself. Of special interest here is the two-way relationship between cyber and ML. On one hand, ML could provide valuable tools for cyber defense and offense. On the other hand, ML technologies in almost all applications are vulnerable to cyber-attacks and thus the cyber-ML systems need resistance to and resilience against such attacks. Development of formal methods for properties at the intersection of cyber and ML is thus an important Cyber S&T topic that cyber and ML experts could investigate together.

3.8 Broader Applications of Cyberspace Technologies: Need for Interdisciplinary S&T

Cyberspace in early days involved computing and networking among people and between people and data servers. As the cyber vulnerabilities of this limited cyberspace were exposed and exploited, cyber defense and offense became a discipline worthy of S&T effort. The expertise in computing, communication, and networking that were key to developing the cyberspace technologies, were also critical for developing technologies for cyber defense and offense.

Over the last two decades, the domains of applications of cyberspace technologies have grown significantly. Almost all commercial and DoD critical infrastructures, vehicular platforms and weapons systems, and healthcare have benefitted from cyberspace technologies. The attack surfaces and consequences of a successful attack could be quite different for these cyber-physical systems, compared to those for traditional computing and networking. Also, the cyber and physical parts of these systems are not easily separable during the analysis and mitigation/weaponization of vulnerabilities. Cyber expertise by itself is not enough to address these new challenges and opportunities at the intersection of cyber and physical. Interdisciplinary S&T using expertise in both will be critical. Commercial and defense industries have been asking for this approach for some time.

IoT brings a different set of applications and interrelationships with cyber. A whole new set of interrelationships will emerge with integration of cyber, physical, neuro, and bio. Again, interdisciplinary S&T involving a wide range of expertise will be needed.

Cyberspace technologies are also getting strongly intertwined with Machine Learning (ML) technologies as well as with the domains of applications of ML. Once again, challenges at the intersections of cyber, ML, and domain of application of ML are important S&T areas that will require interdisciplinary approaches.

Finally, the relationship between hardware and software in cyberspace technologies is changing and cyber will have to look at them together for defense and offense. Interdisciplinary S&T between cyber and microelectronics will be needed to address the challenges at the intersection.

The above discussion motivates four important categories of S&T at intersections.

a. Cyber and domain of application of cyberspace technologies. Each domain can bring its distinct challenges
b. Cyber and ML
c. Cyber, ML, and domain of application of ML
d. Cyber at software-hardware interfaces

Note that each of the above is a category of S&T topics. In addition, ‘a’ and ‘c’ include a set of topics each for multiple domains of applications. Each category includes Formal Methods, discovery and analysis of vulnerabilities, mitigation/weaponization, situation awareness and controls. In absence of focused attention to the challenges and opportunities at the intersections, major gaps could remain in defense and offense capabilities.

3.9 Microelectronics and other 'Hardware Technologies'

It is not an exaggeration to say that the phenomenal rates of advances over the last five decades in almost all cyberspace technologies and their applications have been enabled by the advances in microelectronics, in particular, CMOS IC technology. These advances can be captured by two major observations: Moore's Law and Dennard Scaling. Moore's law is the observation that the number of transistors in a dense integrated circuit (IC) doubles about every two years. Cost per transistor goes down accordingly. Today, a grain of rice costs 7600 times as much as a transistor that is made with 7 nm technology. And the world produced 10,000 times as many transistors as the grains of rice! Dennard Scaling states, roughly, that as transistors get smaller, their power density stays constant, so that the power use stays in proportion with area; both voltage and current scale (downward) with length. Thus, the clock frequency can be doubled every two years without significantly increasing the power consumption. Collectively, these exponential improvements in key metrics have enabled exponential growth in computing speed, memory size, and communication speed. It has also fueled exponential miniaturization, reduction in cost of unit computing speed and storage. Modern networking, computing, software, and myriad of applications could not have been realized without these advances.

Another important development was the Instruction Set Architecture (ISA) that provided an abstraction layer between microelectronics (hardware) and software stack above ISA. The contract provided by ISA allowed software stack to be oblivious to the technology used in hardware and implicitly trust the hardware.

Unfortunately, this march has been slowing. Both Moore's law and Dennard Scaling are effectively 'dead', Dennard Scaling somewhat more so and for a longer time. Density increase is now slower than doubling every two years. Power consumption and heat dissipation issues prohibit increasing clock frequency at historical rates. The overall improvement in cost-performance gains in going from 7 to 5 nm and 5 to 3 nm are in the 10 % range rather than doubling. And the cost of establishing the next generation foundry is becoming prohibitive. The industry that has been used to exponential improvements by shrinking the line width, now need other innovations to keep getting the cost-performance gains. In near and mid-term, the industry is focusing on architectural and design innovations to achieve these gains. Below is a short discussion on some of those innovations and their impact on cyber.

Currently Samsung and Intel have capabilities for 7nm and 10nm. However, TSMC started mass production of 5nm products in 2020, which is the most advanced in the industry. They have also budgeted $20 billion for a 3nm fab. Intel recently delayed its new process, causing it to fall further behind TSMC and Samsung on this front. The amount of work and cost to get to the next smaller size is increasing dramatically, limiting who can do the jump to the next node. Maybe only TSMC

3.9.1 Innovative IC Packaging

Many manufacturers will rely on more innovative IC package solutions, often integrating several already proven functional IC elements within a single IC package.

Integration of heterogeneous devices in an IC

- Innovative packaging now allows multiple smaller pieces of silicon components to be assembled into a single package (chip). These components could be soft or hard IPBs or chiplets and they could be from multiple sources, use different generation technologies, and serve different functions. Thus, the most expensive technology (for example, 5 nm today) could be used for critical chiplets that get the most benefits, chiplets could be reused in other assemblies, and the whole process could be like using Lego pieces to build new products.

"Heterogeneous packaging is really the future. For the next several decades it is going to last. The race in heterogeneous packaging integration got started a couple of years ago. Every semiconductor company is scrambling to beat everybody else. That is going to create a mixture of domain specific architectures. 3D die stacking is going to be phenomenal in its potential for the future." – Dr. Aravind Dasu, Intel Corporation

- A single chip may have a mix of ASICs, CPUs, GPUs, and FPGAs elements. This capability allows an easier, faster, and less expensive way to build SoC. New processors can be designed quickly, and chips can be designed with varying degree of programmability.
- Given industry attention, the capabilities for integration of multiple types of devices in a substrate will keep on improving.

3D IC packaging

- 2D Ball Grid Array (BGA) and Chip-Scale Package (CSP) Technology
- 2.5D BGA. Uses multiple silicon elements mounted on a high-density intermediate substrate (no die stacking)
- 3D multi-die and stacked package solutions

These allow further freedom in integration of heterogeneous devices from multiple sources while also providing miniaturization and faster development. 3D designs and manufacturing use already proven technologies. They also offer: reduced component sizes; reduced power and increased speed; shorter interconnection paths; die sourcing flexibility; pre-testing of die elements for 3D multi-die solutions; unlimited functional configurations; and faster development. On the other hand, the heat dissipation remains an issue.

Both heterogeneous integration and 3D packaging allow flexible sourcing and rapid development of domain specific (e.g., machine learning and AI) packages. Various types of accelerators can be built into the chip. On the other hand, sourcing from multiple foundries creates new challenges for integration and testing, resulting in the following S&T goals.

a. Verification and trustworthiness of heterogeneous chips, possibly with 2.5/3D stacking
    - The least secure foundry determines the overall trustworthiness. For some third party components, it may be harder to even identify the foundry where it was produced.
    - While 3D multi-die stacked solutions allow full testing and verification of individual layers, the other integration technologies allow comparison of electrical properties only for the individual chiplets.

On the other hand, heterogeneity and 3D enable some new techniques for cyber defense:

b. Silicon elements (e.g. chiplets) and software to monitor the entire chip. A trusted chiplet could be inserted in the package to monitor the overall functioning of the chip and send alert or act to minimize harmful behavior. DARPA SPADE program has started exploring this approach and results should be looked at seriously.
c. Obfuscation of design and protection against unauthorized modification. The ability to get individual chiplets from different foundries could allow the use untrusted foundries in building a trustworthy chip. The idea is to design chiplets and layers in such a way that the subset of chiplets sourced from any untrusted foundry could not reveal the overall functions and intellectual property. Also, any design modifications will be evident when assembling into the full package. The individual chiplets could be functional components or non-functional components.

3.9.2 Increased Use of FPGAs and Added Programmability

FPGAs are a class of silicon devices that can be configured by the end-user to serve a variety of purposes. ASICs and general-purpose processors like the CPU, GPU, and TPU power much of modern electronics. Those devices have their capabilities permanently etched in silicon at the point of manufacture. On the other hand, FPGAs feature programmable logic blocks that can be configured by the customer after manufacturing to solve virtually any specific, computable problem. Industry FPGA technology has been trending towards faster and bigger chips running with less power, and shrinking development schedules. On the other hand, ASIC development and fixed portion of manufacturing costs are both increasing, thus making FPGAs more attractive for many applications. Another driver for the increasing interest and use of FPGAs in place of ASICs or Application Specific Standard Parts (ASSPs) is the fact that FPGA applications have become much easier to develop as new, higher-level language-based development flows. For examples, the C programming language, the MathWorks' MATLAB programming language, and numeric computing environment are becoming mainstream. They enable developers to approach FPGA development from a more familiar, abstract perspective. Compared to CPUs and GPUs, FPGAs programmed to carry out specific functions are much faster and more efficient. Because FPGAs are programmable, changes could be implemented rapidly without redesign and remanufacturing. Thus, they have become popular in countless applications where moderate volume and changing nature of the solution prohibit the use of ASICs and ASSPs, but narrow nature of application makes FPGAs faster than CPU and GPU. Some examples are: Software Defined Radio (SDR); search algorithms; machine learning (ML); encryption; compression; data analytics; and countless accelerator functions.

> *"Many projects are converting from ASIC to FPGA. Users are now expecting tool robustness as with ASIC tools. Some applications that could only use ASIC can now be implemented in FPGA" – Danial Platzker, Product line director of FPGA Synthesis at Mentor Graphics Corp - from publication: Changes in ASIC Landscape Opportunities for FPGAs*
>
> *"The FPGA market is clearly poised to enable replacing a lot of SoCs (System on Chip) and ASSPs by off-the-shelf FPGAs, which at the advanced silicon nodes will offer the complexity and power efficiency needed to support many applications in the consumer, automotive and wireless markets. Also, in some of the traditional network infrastructure markets FPGAs can take on a bigger role through a combination of optimized signal processing IP blocks together with processors on a single chip" – Dr. Johannes Stahl, VP and GM of CoWare's DSP Solutions Group - from publication: Changes in ASIC Landscape Opportunities for FPGAs*

Microsoft has championed the use of Verilog to program an FPGA for classes of applications, effectively creating multiple specialized FPGAs from one FPGA and making user programming much easier. This layer also allows ISA to be changed frequently, if desired. Heterogeneous packaging and 3D allow FPGAs to coexist in a package with ASICs, CPUs, and GPUs, thus allowing complex SoC in one package.

The following are some challenges and opportunities:

a. Protecting FPGA programming information stored in external memory (at rest and in transit): FPGA devices are volatile, i.e., they are typically programmed/re-programmed through an external (memory) device. An adversary could steal or alter the bit stream stored in these devices.
b. Ensuring the trustworthiness of third party and open-source software introduced in FPGA middleware. When FPGA is programmed to create classes of FPGAs, another layer of software is added between hardware and user programming. Industry practice will allow open source and third-party products to be used in this software, thus creating new attack vectors.
c. Technologies inserted in the FPGA middleware to monitor FPGA activities for anomalies
d. Diverse and dynamic FPGAs to provide new SDD and MTD techniques. The intermediate layer could be used to create 'changing FPGA', thus providing a moving target to the adversary. Also, different systems could use different versions, thus allowing SDD.

3.9.3 FPGAs and Heterogeneous Packages

When FPGAs are parts of the complex heterogeneous packages discussed in Section 3.9.1, the whole package becomes programmable System on a Chip (SoC), providing several benefits.

- Custom processors and soft processors can be implemented easily
- Domain specific architecture and ISA could be implemented easily. An example is ML FPGA embedded in a SoC.

- Many kinds of accelerators can be added to assist CPUs and GPUs
- With built-in analytics, the whole circuit could be made self-evolving.

With the heterogeneity, softwarization, and programmability added to what used to be an unchangeable monolithic hardware, there will be increasing number of moving parts and cyber vulnerabilities. The programming process, third-party software and chiplets, and interrelationships among chiplets in the chip could create vulnerabilities that could be used to exploit the whole chip. New side channels could result from bringing dynamics down to the chip level. On the other hand, it is now possible to add intelligent monitoring and analytics (including ML) down to the chip level. These could not only identify vulnerabilities from software programming but could also identify vulnerabilities in ASICs and processors from natural sources and Trojans.

Thus, the following are important new S&T goals:

a. Trustworthiness of IPBs, chiplets, and the entire chip, including the impact of third party chiplets and software
b. Identification and mitigation of new side channels
c. Self-monitoring chips using programmable FPGA to identify vulnerabilities from software as well as from ASICs and processors. Chip level ML could be used for the analytics.

3.9.4 Blurring of the Boundary between Hardware and Software

The changes discussed above in Sections 3.9.2 and 3.9.3 blur the traditional boundary between hardware and software provided by the ISA as an abstraction layer. The contract between software and hardware implemented by ISA is in jeopardy because of this blurring. New side channels add to the blurring. Software stack may not be able to ignore microarchitecture for overall trustworthiness. One approach is to create a different abstraction layer that allow higher layers to be oblivious to the layers below the abstraction layer. This would allow independent verification of the trustworthiness of layers below and above the new abstraction layer. Another approach is to verify hardware and software jointly. The following S&T goals are thus important:

a. Identification and mitigation of new side channels, especially those that add to the blurring of the hardware-software boundary
b. Identification, design and verification of a true abstraction layer that could provide a non-porous boundary
c. Techniques for joint verification of hardware and software, at least the interface layers

3.9.5 CMOS 3D Near Memory

In general purpose computer (Von Neumann) architectures the bandwidth of data to and from memory (commonly referred to the "memory bottleneck") limits computation performance. Monolithic integration of additional logic and memory in the wiring layers of CMOS device circuitry can dramatically increase the memory access bandwidth, providing performance improvements of up to 10x.

3.9.6 Beyond CMOS Microelectronics

Research in several directions is being pursued to circumvent the limitations of CMOS manufacturing. However, it may be decades until any of the research comes to fruition and hence Cyber S&T may be far into the future. Here, we simply list key directions being pursued and should be watched for any breakthroughs that could speed up the technology TRL.

- Tunnel Field-Effect Transistor
- Magnetoelectric (Spin-based) technologies
- Superconducting technologies
- Nanomaterials like Graphene
- Biological materials

3.10 Networking and Communication

Communications and networking technologies, their applications, as well as their control and management could see significant changes in the next two decades. Even accounting for the hype, the changes are likely to be significant enough to have major impact on the personal and professional lives as well as military conflicts, especially in conjunction with other technologies such as IoT, ML, Cloud Computing, Edge Computing, and device miniaturization. The changes in communications and networking will bring many new cyber challenges and opportunities that cyber S&T will need to address.

Some other factors make it even more important to take a serious look at the likely changes in communications and networking, and impact on cyber defense and offense:

- The rate of growth of the maximum data rate per wavelength (that is the maximum line speed) is slowing due to the constrained imposed by physics. Going beyond 5 Tbps per wavelength will be exceedingly difficult. This slowdown has two important consequences for the future networks. First, very large data transfers will be efficient over short distances (10 km – 100 km) and will rapidly decrease in efficiency as the distance increases. The second impact is that more channels (wavelengths) will be packed in the network infrastructure and inverse multiplexing will be used to get high point to point data rate. This will have an impact on the routing protocols and edge caching as data sets must be reassembled from distributed communications paths."
- The commercial industry now drives almost all deployment of major advances in communications and networking technologies. DoD tactical wireless networks have been major exceptions so far. It is not clear that this independent development and deployment will continue with mmWave and THz communication or the next generation DoD tactical networks will be relatively minor adaptation of commercially developed and deployed 5G/6G technologies. The former could be prohibitively expensive, and the latter will have the same technologies available to all our adversaries. Cyber defense and offense could now be time race in finding and fixing vulnerabilities, developing cyber weapons, etc.
- The USA does not have leadership in developing and standardizing key new technologies, especially new wireless access (cellular mobile) technologies. Combined with the loss of the leadership in manufacturing state-of-the-art microelectronics that feed key components of the next generation cellular mobile communication, the overall change in leadership is dramatic. This change could give a head start to adversaries in the race for cyber vulnerability discovery and mitigation/weaponization. It could also give adversaries an advantage in technology customization and cyber defense.

3.10.1 Future of Internet

For at least the last two decades, Internet backbone infrastructure has remained essentially unchanged. TCP and IP protocols, structure of autonomous systems (ASs), routing within and between ASs, reasonably open connectivity, and cooperative management have characterized Internet even as the number of users, data capacities, and services have mushroomed. Per user data requirement is reaching a plateau. Of course, the number of humans and devices on the network keep on increasing and the latter will dwarf the former during this decade.

More fundamental changes could happen in the next two decades.

Network Connectivity, Balkanization/Splinternet

Cyber vulnerabilities and their exploitations, Government concerns with openness, differing policies regarding data privacy, and a desire for clandestine activities could change the Internet connectivity model. Some possibilities are discussed below.

- Internet remains ubiquitous and more or less fully connected with reasonable control of cyber events (more secure version of the current Internet). VPNs and other mechanisms allow serious commerce and Government business to be carried out on this Internet.

- Internet remains ubiquitous but not secure enough for serious commerce and Government business, resulting separate private networks and organizational Balkanization.
- Political leadership in some countries decide to isolate their parts of Internet from the global Internet and introduce severe access and egress controls, thus resulting in national/political Balkanization.
- Varying privacy and data sharing requirements in different countries may lead users to semi-Balkanize Internet.

The following S&T goals are motivated by the above discussion. In the table below, the entries 'a' and 'b' are contingent on observing a strong trend towards Balkanization.

a. Cyber SA in Balkanized Internet will be a challenge and an S&T goal
b. Access to adversary systems for ISR and cyber offense is another S&T challenge

Routing and other protocols

Current routing protocols could continue to serve the Future Internet. On the other hand, data, information, and content centric routing and information storage (Content Based Networking or CBN) have been studied well and offer many advantages now that information transfer, storage and retrieval dominate the Internet usage. It is conceivable that these protocols become mainstream rather than an overlay in the Future Internet. If Internet does get Balkanized, some 'islands' may decide to use CBN while others may continue with traditional routing. These are massive changes with serious implications to the infrastructure.

While well studied, CBN uses new and 'untested' protocols so the initial period could be challenging for cyber defense. Another area of concern is the storage (cache) of data and information at many places in the networks, as opposed to at the user site and large commercial database sites. A greater number and types of data storage will have to be protected against privacy, confidentiality, and integrity violations. Innovative data access controls will need to be designed. On the other hand, Zero Trust Strategy and Edge Computing will mandate trustworthy CBN. Similar trustworthiness will be required of the new protocols developed to manage limits on the per wavelength data rates. Sophisticated tools to carry out vulnerability analysis, mitigation, and formal verification prior to deployment will be required to achieve this trustworthiness.

Thus, the following S&T goals are relevant.

c. Techniques to protect distributed databases scattered through the network
d. Security verification of all new protocols

Control and Management

Significant changes are likely in the control and management of Internet, large private networks, and infrastructure for cellular wireless networks. One is centralization and varying degree of separation between data and control planes via Software Defined Networking (SDN). Second is very flexible implementation of networking functions via Network Function Virtualization (NFV). Together, they offer softwarization, programmability, and dynamics. They also facilitate automation and use of ML techniques in control and management.

Software Defined Networking (SDN) and Network Function Virtualization are two different concepts but are frequently and erroneously lumped together. Both create opportunities and challenges for cyber and hence S&T needs.

SDN refers to the ability to dynamically set up, tear down, and reconfigure provisioning, protection paths, routing information, and path computation via software from a centrally managed location. On one hand, centralized control and management enable much better situation awareness and deployment of consistent management and security policies, updating them consistently across the entire domain managed by an SDN controller. Software agents could be deployed to automate configuration and eliminate human errors. ML could be used more effectively from within a single controller. However, SDN controller is a single point of failure and a big target for cyber-attacks. Thus, while isolated SDN controllers have been in use for a while, the architecture for SDN controller network could use serious S&T. This S&T should evaluate benefits of federated and federated-hierarchical arrangements of SDN controller network with designed redundancy so each network entity could be managed by more than one SDN controller. It should also look at the network of SDN controllers that can self-monitor member SDN controllers.

NFV allows a common hardware to be used, with appropriate software, as one of many network appliances – routers, WAN accelerators, encryption devices, switches, NAT and DNS controllers, etc. Common hardware greatly improves maintenance concerns. However, the biggest advantage is the ability to distribute network appliances to where and when they are needed, and then dynamically redistribute as the needs change. This capability is critical for functionality of 5G networks. In addition, using virtual machines (VMs) and/or Containers, a single hardware device could provide multiple virtual hardware devices, each providing one of the above network functions. In addition to the flexibility and efficiency, NFV and SDN together could provide redundancy, diversity, and dynamics to thwart a cyber-attacker.

Currently, control functions have been automated to varying degrees, while management functions have much higher manual component. With softwarization, centralization and virtualization, it is easier to use analytics to automate both sets of functions further and improve the efficiency and security. Automation and possible use of ML come with new attack vectors and ability for the adversary to inflict massive damage when a centralized control and management system in an SDN controller is compromised. The analysis and mitigation/weaponization of vulnerabilities should be an integral part of the S&T leading to the automation of control and management functions in the future Internet and large private networks.

The following are some S&T goals motivated by the above discussion.

e. Cyber defense enabled by centralized control and management. Use of ML. Superior Cyber SA.
f. Autonomic and autonomous resilience using SDD and MTD enabled by NFV
g. Resistance and resilience using the right architecture for the network of SDN controllers and their relationship with data plane assets

Within the next decade, we may lose complete visibility to all traffic on the Internet including packet headers, dramatically increasing the difficulty doing surveillance of our communications networks-Professor C. Cotton, University of Delaware

At application level, migration to web services implies that most traffic on the network will be https. Zero Trust strategy will add new encryption layers. Together, they will make in much more difficult to monitor the network traffic. This motivates the following S&T goal.

h. Scalable technologies to enable monitoring https and otherwise encrypted traffic

Note that there is a large degree of uncertainty in ‘if and when’ for ‘a’-‘d’ above.

3.10.2 Increasing use of air/space-based platforms

Most commercial communication and networking infrastructure is land and underwater based, with satellites performing significant broadcast communication and limited full communication for hard-to-reach areas. DoD has been using space-based platforms for communication and networking for a long time. However, the space platforms have performed minimal networking functions. The situation is likely to change. Rapid commercialization of Low Earth Orbit (LEO) satellites has the potential to provide ubiquitous high bandwidth communication to areas of the earth where density and economics do not justify wired infrastructure. Thus, all inhabitants of the planet and their devices could have high speed access to communication and networking. The LEOS providing these capabilities will have full networking capabilities. DoD will benefit from these developments since they will then have full networking capabilities in space-based platforms and can build space networks serving both ubiquitous access needs and a higher-level backbone for terrestrial networks. Of course, having these networking functions in space-based platforms will create new attack vectors with cyber or EW based access.

a. Defense of space nodes against Cyber-EW attacks
b. Secure update technology for space nodes.

3.10.3 Evolution of Cellular Wireless Networking Technologies and Tactical Wireless Networks

Historically, commercial cellular wireless technology generations are about a decade long. Each starts with major claims compared to the prior generation, but it may be halfway to the next generation before the current generation reaches full maturity and deployment. Currently, the industry is touting 5G as a major step from 4G and 5G label is affixed loosely to the service offered to a customer. Already academic and some industrial research activities have begun for 6G.

3.10.3.1 5G

In terms of per user data rates, 5G is a natural jump from 4G. However, some changes from 4G to 5G are more fundamental and those may create significant new cyber challenges and opportunities. A short discussion follows.

a. Geolocation. With mmWave range 5G services, cell sizes could shrink, and spectrum reusability could increase with sophisticated spectrum management and power controls. This cell size shrinkage will permit high end-user (human and device) density, thus supporting the IoT vision of very large devices/humans ratio. On the other hand, this shrinkage could have an impact on non-cooperative geolocation capability. Alternatively, longer distances can be served using narrow beam forming antenna, once again impacting geolocation and other EW techniques.
b. Device and network architecture-based security solutions for high density device-device communication. Since 5G will support much higher fraction of device-device communication, devices, some with low SWaP, will need cyber defenses against a large spectrum of cyber-attacks. Some experts feel that most low SWaP IoT devices are will not be able to provide the required cyber defenses in absence of a major S&T push to develop innovative solutions. More detail on this presented as part of the discussion of IoT.
c. Use of lean design techniques for cyber defense. 5G will use lean design techniques where communications between the end user and network are limited to on-demand and not always on. This provides energy efficiency for network equipment serving large number of devices and for low SWaP devices themselves. It could also provide defenses against cyber and EW attacks.
d. Cyber defense of dynamic controls that provide a wide range of services with decreasing use of HIL. Compared to 4G, 5G standards promise a wider variety of services in terms of QoS metrics and data rates. They also offer a greater degree of user programmability of services. Network slicing and other mechanisms will be used to deliver these differential services. Sophisticated measurements and algorithms will be required for using these mechanisms effectively. ML techniques could play significant roles. In the beginning smart algorithms and ML could be run offline to help configure the network. Over time, these tools could get transformed into real time intelligence providing automated QoS management, possibly using software agents. Increasing use of machine intelligence with little or no human involvement will bring new attack vectors and risks.
e. Use of built-in levers to maximize cyber security of increasingly open and programmable infrastructure. Compared to 4G, 5G architecture has greater decoupling between hardware and networking software, greater roles of software, greater flexibility in where processing for various services may get done, and greater programmability. With openness and flexibility come new attack vectors that need to be understood, researched, and mitigated. On the other hand, there is greater awareness of the cyber vulnerability in the 5G community and even among large hardware suppliers. Thus, levers are being inserted to enable sophisticated monitoring and real time actions for cyber defense. Focused S&T is needed to take advantage of these new capabilities to balance security and flexibility, for carrier networks as well as networks in commercial/industrial campuses and military bases.
f. Architecture for data collection and analytics to support network management and Cyber SA. Smaller cells and high user density will result in high user and network control data. Most user data will be transiting short distances. Analytics on the network data for network management and cyber situation awareness will be a challenge. On the other hand, localization suggests that federation and hierarchy in analytics may be attractive for scalability. Edge computing, facilitated by 5G, could be useful.
g. Managing the loss of supremacy.

h. Architecture and design of DoD's future tactical wireless networks and associated cyber defense. As mentioned earlier, tactical wireless networks used today by the DoD in general, and Army in particular, are quite different from the commercial cellular networks. In the future, the DoD tactical networks will add higher data rate capabilities using mmWave and THz spectrum. Given the high cost of architecting, designing, and implementing fundamentally new tactical wireless technology, it is possible that the DoD may decide to adopt 5G with some modifications that are not prohibitively expensive but offer additional desired features and security. Deployment of tactical networks based on open standards has many advantages in terms of cost, technology updates, and security updates. However, there could be serious implications for winning future battles of cyber defense and offense. It will be important to add the right amount of 'secret sauce'.

3.10.3.2 6G and Beyond

Even though full 5G adoption is many years away, there is already a significant amount of work by academia and industrial laboratories on the follow-on technology for 6G and beyond given the desire to deploy the next generation in the next decade. Even though it is early, the following features seem highly likely to be present.

- Expanding the network virtualization to the full stack
- Slicing to a much greater extent than 5G
- THz frequencies and hence very narrow, highly directional, high gain antennas for reasonable distances
- Very high degree of spectrum reuse using small cells
- Increasing use of ML in controlling and managing the network and spectrum, especially for small and very dense cells.
- New sets of applications involving precision sensing (e.g., haptic sensing), remote medicine (including surgeries), precision positioning and timing, machine to machine high quality video communications, and maybe holographic video communication.
- Novel human-machine and human-human communication methods. In conjunction with continuing explosion of the number of networked devices and integration of human brain and silicon, 6G data rates and latency could lead to instant human to machine and human to human communication without using intermediate machine language by transmitting brain waves.

At a high level, it seems that 6G will have similar set of cyber challenges for the infrastructure and core services as 5G but with much stronger consequences. Two areas where the concerns are even larger are the expected heavy use of ML and some applications that are extremely sensitive to cyber-attacks.

3.10.4 New communication Media: VLC/LiFi, Free Space Optical Communication

Visible Light Communications (VLC) using next gen LED lights can provide the high bandwidths needs for advanced 5G and 6G applications. Coupled with LiFi technologies, VLC will enable LPI/LPD communications over short ranges up to a few kilometers. Another important attribute is that these technologies are difficult to geo-locate making them very useful in dispersed command post and distributed command and control applications. Free space optical communication can provide high data rates over long distances but is sensitive to fog and other weather-related issues.

Since most work to date has been on transmission of signals, real communication and networking protocols are still to be designed. Thus, the following are three high level S&T goals.

a. Use LPI/LPD naturally available to develop defense against CYBER-EW attacks
b. Develop Cyber-EW offense that works despite the LPD/LPI properties of these new media
c. Actively participate in the design of architecture and protocols, evaluate from cyber perspective, and build-in security features.

3.10.5 Multi-Technology Networking

Several wireless technologies providing extremely high data rates are susceptible to weather conditions. Thus, rain and fog affect mmWave and free space optical communications, respectively. In addition, extremely high service availability is critical for the DoD tactical networks and, increasingly, nation states have the ability to compromise large portions of the network. Given the above, it is likely that the future networking will be supported by multiple networks with different communication media and even different networking protocols. Also, these networks will be managed as a single entity and workload may be distributed based on the status of each component network and the service requirements of the user applications. On one hand, the redundancy and flexibility could be a tremendous enabler of high reliability and high availability operations. On the other hand, added management complexity and new interconnections could open new attack vectors. The following are some important S&T goals.

a. Cyber diversity (software, protocols) in addition to physical redundancy
b. Highly reliable and secure control mechanisms that monitor the component networks and assign workflows

3.11 Computing

3.11.1 Core Computing Technologies and Architectures

Over the last decade, multi-core processors and GPUs have enabled tremendous gain in computing performance for an array of applications and enabled scaling many algorithms (e.g. DNN, DRL, and large-scale simulations). TPUs promise to provide even faster processing and lower power consumption for inference workloads. Again, large scale simulations, many algorithmic techniques, and ML will benefit greatly. Combined with accelerators in chips, the computing capabilities for all analytics will see major gains in this decade and likely continue into the next decade. They will also enable sophisticated tools for cyber vulnerability discovery and mitigation/weaponization, leading to increasing automation of the entire process. The following are resulting S&T goal.

a. Use of the emerging computing capabilities for accuracy, scalability, and automation of cyber defense and offense. ML could provide an important means to reduce the required effort from human experts. Of course, the trustworthiness of ML is a challenge to be addressed for this promise to be realized.

Other important trends in core computing are programmable processors, custom processors, and heterogeneous architectures. Heterogeneity will permit new cyber defenses using SDD and MTD. Custom and programmable processors will make it harder for adversary to find vulnerabilities because of difficulty in accessing specific instance deployed and executing at a given time. On the other hand, every customized/programmed version will need to be evaluated for vulnerabilities that should be fixed before fielding, a cyber-defense challenge. These lead to three S&T goals.

b. Use of programmability and customizability of processors to make it harder for the adversary to find vulnerabilities in the instance deployed
c. Use heterogeneity of microarchitecture and ISA to develop new SDD and MTD techniques
d. Quick verification techniques to evaluate new instances for vulnerabilities. In particular, techniques that allow incremental verification may be useful.

Over a longer time frame, it is conceivable that biological computing and storage will mature and enable even faster computing. Similarly, over a long and uncertain time frame, Quantum Computing may become real beyond the ability to break asymmetric encryptions. These are discussed separately.

3.11.2 Cloud Computing

Cloud computing refers to the use of remote virtualized servers hosted by one or more cloud service providers to store and process data, instead of using one's own servers or personal computers on premises. In addition to many services like emails and file storage provided directly to consumers, many cloud service vendors provide a variety of services to businesses of various sizes. The migration to cloud based computing is growing. The trend towards 'almost anything as a service' from the cloud will continue because of economics. Businesses also use hybrid clouds where an on-premises datacenter (private cloud) and remote servers (public cloud) share data and applications (processing) between them. Many businesses use a 'multicloud' arrangement where public clouds are provided by multiple providers. They may share data and processing with a private cloud. Inexpensive high-speed communications and massive storage capacities in public clouds enable transparent services to the end users, while making the best computing technologies available affordably. Hybrid multi-cloud arrangement enables redundancy, while also allowing the most sensitive data and processing to be kept on the private cloud. In addition to businesses subscribing to cloud services, telecom service providers (especially cellular providers) are benefitting from cloud type arrangements in their own infrastructure.

Government in general and the DoD in particular are lagging in the use of cloud computing, but the usage is increasing. Frequently, several Government organizations decide to share a 'public cloud' only among themselves when sharing data and processing are advantageous.

Increasing use of cloud services and new ways in which the cloud service providers create and provide innovative services lead to many challenges and opportunities for cyber. Some are discussed below.

3.11.2.1 Exascale Computing for All: Democratization of High-End Computing

One major impact of the cloud services is democratization of secure high-end computing. Any organization can get access to secure computing resources and software comparable to those available to affluent nation states. Adversaries with modest means are just as capable of addressing complex problems and projecting force in cyberspace as we are. The following discussion details the democratization and challenges posed.

Recently, graduate students at UCSD leased 52,000 GPU accelerators on multiple clouds to demonstrate Exascale capability. Such capability could be used for sophisticated physics simulations (weapons, energy, chemicals) and data analytics (patterns of life, text mining, "needle in a haystack"). Combining access to high capacity and high-speed computing resources with the vast libraries of high-quality software available for free online, it would be relatively straightforward for non-state actors to implement ML, conduct surveillance, mission planning, and counterintelligence operations using publicly available and commercial datasets. They will be able to carry out all these activities with stealth enabled by cloud service providers. New and emerging security features in cloud services will continue to improve stealth and help these players in clandestine activities. These new types of activities are thus going to be more difficult to monitor using conventional means. Many third-party advertising and tracking firms that retain sensitive data about US personnel that could be easily accessed by non-state actors for hypertargeting. In addition, access to world class computing resources enable the actors to develop new cyber, EW, and kinetic weapons of terror. The above observations motivated the following sets of S&T goals:

a. Technologies that are effective on adversaries using professional cloud services
b. Leveraging the cyber defense techniques in public clouds to get better cyber defense in private clouds for the DoD mission critical data and services

3.11.2.2 Cloud Computing, Privacy, and Cyber Defense

Remote storage and computing services provided via private and public clouds, hybrid clouds, and multi-clouds result in efficiency, cost savings, redundancy, and access to most advanced algorithms and analytics. They could also afford and provide the best cyber security measures and update them as better ones arrive. Cloud service providers insist that moving all sensitive data, processing, and authentication to the cloud is the best approach for cyber security. They point to the fact that recent serious breaches (e.g., Solarwinds) could have been avoided if all services were provided

> *"We refuse to do an on-prem version of our products. We only work cloud and that is where I think we should really be, by staying steadfastly focused on having a SaaS model, it set us up for success. We are in Gov Cloud and we're in different regions for different privacy issues with European clouds." – Adam Meyers, Crowdstrike*

by clouds. In fact, cyber defense itself is now offered as a managed services (i.e., Crowdstrike). The access to organic customer data affords better threat intelligence to these providers for all subscribing customers. The cost-performance benefits of this model will continue to disincentivize isolated on-prem installations.

On the other hand, centralization of data and computing services using shared resources could lead to potential loss of privacy, massive data and intellectual property breaches, and denial of service due to massive outages from natural and malicious causes. Vulnerability increases significantly when processing is used as a service from the cloud, since the data is typically decrypted while processing. Additionally, services provided by the cloud could be hijacked and corrupted, affecting many users simultaneously.

> *"More broadly, independent of what security standard you use for this kind of authentication, the thing that we have been advising our customers and the practice that we have been following ourselves is to do the following. 1: move your authentication into the cloud. 2: Secure all your devices. 3: make sure you are using multifactor authentication. 4. Make sure you have least privileged access. 5: Use a contemporary antivirus or antimalware service … The reality is that any organization that did all five of those things, if it was breached, it in all likelihood suffered no consequence" - Brad Smith, Microsoft (in testimony to the Senate Intelligence Committee regarding the Solarwinds hack.*

A mix of operational policies and technology solutions will be needed to achieve the right balance and desired risk-benefit profile. Some technology aspects are discussed below.

3.11.2.3 Mix of end user, private cloud, and multicloud arrangement

The user organization could distribute the data and processing between the end user terminal, private cloud, and one or more public clouds. Multicloud certainly offers redundancy but adds management burden on the user organization. User terminal and private cloud offer privacy and confidentiality of sensitive data and a degree of service availability in the event of cloud failure. However, the user organization now needs to manage data storage and software acquisition and updates. Recent well publicized attacks (e.g., Solarwinds) have shown the difficulty in securing these channels. Decision makers need quantitative models and tools to help make informed decisions about the mix of private and public clouds, splitting data and workload among available resources, and dynamic movements. Simple economics driven calculations are not appropriate. This motivates an S&T goal.

c. Quantitative methods and tools to design the right hybrid-multi cloud service and dynamic management of workflow among private and several public clouds

3.11.2.4 Virtualization, Microsegmentation, and Microservices

Virtualization using hypervisors allows a single hardware platform to be used as multiple logically separated virtual hardware devices (virtual machines or Containers). In this report such virtual devices are referred to as virtual entity (VE). VEs within a hardware could be heterogeneous. In some applications, many tens of such VEs have been used within one hardware. Interactions between these virtual entities (VEs) are controlled using hypervisor and security policies. Virtualization in private or public cloud provides efficiency and cost savings. It also enables Spatial Diversity Defense (SDD) by having different variants of any required software in different VEs, thus limiting the number of VEs that can be compromised using one vulnerability. Additional security is achieved by dynamically changing the software variant in each VE and by moving the workloads among VEs, thus providing Moving Target Defense (MTD).

The whole process from **Policy, to Orchestration, to Controller, to Devices** can now be automated by the cloud service provider for management policies in general and security policies in particular. Different VEs could have different policy settings. **Microsegmentation** goes even further by enabling security policies to be assigned individually to data center applications, down to the workload level. Security policies can be synchronized with a VE, operating system (OS), or other virtual security targets. Effectively, there is then the possibility of differential security based on application and/or user organization. **Microservices** take virtualization to another level. They are loosely coupled services combined within a software development architecture to create a structured application. The microservices architecture allows the individual services to be deployed and scaled independently (typically via Containers), worked on in parallel by different teams, using different programming languages, and having their own continuous delivery and deployment stream. Going one step further, services can be assembled in real time so different portions of the workflow could be executed at different places, possibly by different providers. Software upgrades, patches, etc. could also be provided as microservices. **Kubernetes** could be used to distribute the workload dynamically to provide scalability and flexibility. Cloud services thus now have a complex supply chain with third parties playing larger roles. 'Software' could be assembled on the fly.

On one hand, virtualization, microsegmentation, and microservices offer flexibility and fine-grained security controls. On the other hand, there are many more moving parts behind the scenes and opacity as to where the workload executes and who secures what. Hybrid clouds, while allowing controls of sensitive data and computing in private cloud, create split responsibilities for management and security in this complex supply chain. Recent massive cyber-attacks (e.g., Solarwinds) have exposed the vulnerabilities of private clouds to supply chain attacks. All these tradeoffs need to be understood objectively and quantitatively. Focused S&T on the mechanisms for late-stage verification and dynamic monitoring will be very important. The resulting S&T goals can be summarized as follows:

d. Identification of the right candidates for generating variants and building SDD and MTD to capitalize on the affordable virtualization and dynamics. Robust orchestration of SDD and MTD.
e. Defense against side channels in general and those impacting SDD and MTD in particular
f. Use of microsegmentation to provide security commensurate with importance of data being protected
g. Control of complex supply chain at all stages of addition and integration
h. Late-stage rapid verification, possibly of binaries assembled from multiple source code suppliers
i. Constant monitoring and detection of anomalies

3.11.2.5 Roles of Encryption in Shared Storage and Computing Environment

Encryption has been used extensively to protect the confidentiality of data in transit and now also the data at rest. Cryptographic protocols allow only the trusted parties to decrypt the encrypted data. Thus, storage in the cloud and transmission between the user and the cloud can be kept secure using encryption. However, there are several situations where this is not enough, and additional technologies and techniques may be needed.

- **Protection of data while processing**: When processing is performed in the cloud, the data is typically decrypted, worked on, and re-encrypted. Exfiltration of un-encrypted data during this period is a significant vulnerability. Two general approaches have been discussed in this context and need further investigations.
    - Provide, to each group of users, a small, trusted area where decryption happens, processing is carried out, and the data is re-encrypted before sending outside. An example is Intel's Secure Guard (SGX). Other similar approaches could work.
    - Process without decryption using homomorphic encryption (HE). HE allows processing directly on the encrypted data. The result of the computation is in an encrypted form and, when decrypted, the output is the same as if the operations had been performed on the unencrypted data. HE is a promising cryptographic technique that protects data in-transmission, at-rest, and in-use.

      There are several types of HEs:
        - Full Homomorphic Encryption (FHE): FHE allows the entire set of mathematical functions to be performed on the encrypted values.
        - Partial Homomorphic Encryption (PHE): PHE allows a limited set of mathematical functions to be performed on encrypted values.
        - Somewhat Homomorphic Encryption (SHE): SHE allows a limited set of mathematical functions – up to a limited complexity – to be performed on encrypted values.

  Currently, FHE has severe performance penalties and limitations on the types of queries or analytical functions that can be run. Intel and other players have achieved breakthroughs in scalability and resource consumption but practical FHE is far from reality. Quantum Computing may provide additional boost to practical FHE. In mid-term future, PHE may provide an acceptable trade-off between security and performance.

- **Multi-Party Computation:** Many organizations want to share their data sets for processing on consolidated data but do not want to share the actual data with other parties in the group. The solution is Secure Multi-party

Computation (SMPC). Formally, SMPC uses innovative encryption (cryptography) to allow parties to jointly compute a function over their inputs while keeping those inputs private. The following are some example applications: Secure auctions; secure voting; and federated secure machine learning. Despite 3-9 orders of magnitude improvements in the past decade, the cost of deployment is still a challenge. The required bloating in computing and communication is the killer. It is an active area of research. Another approach to SMPC is to design computing in a way that allows each party to share a summary of the data and the computation can be performed over these summaries to get the required answers.

- **Private Information Retrieval (PIR) or Privacy Preserving Search (PPS):** Yet another challenge is where a user/organization wants to look at some part of the database (may be owned jointly with other organizations) in the cloud without letting others know what was of importance. This Privacy Preserving Search (PPS) is especially important for coalitions.
- **Differential Privacy (DP):** Systems for sharing information about a dataset (i.e., by describing the patterns of groups within the dataset), while protecting specific datum in those datasets, offer novel approaches to intelligence collection and dissemination
- **Functional Encryption**: Where restricted secret keys enable a key holder to learn about only a specific function of encrypted data and nothing else.
- **Obfuscation:** Sometimes, memory access patterns reveal a lot about the computation being performed. An oblivious RAM (ORAM) simulator is a compiler that transforms algorithms in such a way that the resulting algorithms preserve the input-output behavior of the original algorithm, but the distribution of memory access pattern of the transformed algorithm is independent of the memory access pattern of the original algorithm.

Some S&T goals for the next generation encryptions for cloud computing are as follows:

j. Minimization of decryption even during processing using SGX type solutions
k. Scalable cryptographic computing: PHE and FHE; SMPC; PPS, etc.

3.11.3 Edge Computing

Note that Edge computing, IoT, and 5G feed one another and there is some duplication in the narrative.

Edge Computing implies pushing the frontier of computing applications, data, and services away from centralized nodes to the logical extremes of a network. It enables analytics and data gathering to occur at the source of the data. Edge computing could be performed on large computing platforms, low SWaP IoT devices, or on laptops and smart phones. The following are some key advantages of Edge Computing.

- Low latency
- Reduced data rate requirements for the wide area networks
- Useful computing even when there is no connectivity to wide area network
- Use of idle computing capabilities in devices such as laptops, smartphones, tablets, and a large variety of sensors
- Privacy and confidentiality of data and information
- Use of ML capable chips to build highly fault tolerant and cyber resilient network of ML capable devices

Of course, Edge Computing creates new cyber challenges and opportunities that need to be addressed. The following are some S&T Goals.

a. Constraint aware cyber defense. Customized cyber defenses that are effective but can run on low resource devices.
b. Decentralized trust model

c. Architecture for redundancy, cyber diversity, and rapid recovery so failure or compromise of a subset of nodes does not bring down the mission. Large number of inexpensive devices and high-speed communication enabled by 5G could facilitate such an architecture

We are moving to edge computing, but edge may not be ready in terms of security. Constraint-aware cyber security and computation integrity will remain a challenge –Professor D. Xu, Purdue University

For continuity in narrative, Quantum Computing (QC) is discussed in Section 3.12 as one of the several key capabilities enabled by atomic scale properties.

3.12 Quantum Timing, Sensing, Computing, and Communication

Quantum science is the study of matter and energy at scales that are small relative to fundamental constants of nature. Unique properties of matter and energy at these scales enable many new cyberspace technologies. Key concepts leading to the promises of breakthrough applications are quantum bits or qubits, superposition, and entanglement. After decades of fundamental research and prototyping, some feel that we are approaching an inflection point and that 2021-2030 could be a quantum decade in which some impactful applications will be deployed, leading to a wide variety of applications in the 2031-2040 timeframe.

Breakthrough advances in timing (atomic clocks), sensing (quantum sensors), computing (quantum computers), and communication (quantum communication) could result from exploitation of the key properties of matter at quantum scale. These advances could translate to significant new and improved capabilities for the DoD:

- Precision positioning, navigation, and targeting (PNT) in denied environments
- Intelligence, surveillance, and reconnaissance (ISR)
- High performance computing for some types of problems; and
- Secure cryptographic solutions for military communication

The DoD Quantum Roadmap discusses the technology readiness levels and future directions for Atomic Clocks with increasing accuracy and SWaP-C, various types of quantum sensors, quantum computers, and quantum communications.

3.12.1 Timing

Overall, atomic clocks are at an advanced state of maturity and can provide distributed synchronized timing with nanosecond (ns) accuracy now. By 2030, this could improve to picosecond (ps), about a thousand times more accurate than Global Positioning System (GPS)! Synchronized distributed timing is critical for many commercial and DoD applications like PNT. It is therefore important to invest now in evaluating and mitigating vulnerabilities in the basic mechanisms and to help develop an ecosystem that minimizes the attack surface, especially at the interfaces between the timing mechanism and the applications. It is also important to identify if the basic timing mechanism allow greater resistance to cyber and EW attacks than the non-quantum clocks do. Thus, the following two S&T goals.

a. Mechanisms to prevent timing attacks on atomic clock and to build resilience in the eco systems to maintain timing despite a compromise
b. Technologies for Cyber-EW attacks on atomic clocks.

3.12.2 Sensing

Quantum properties allow various types of sensors with high precision and sensitivity but in narrow bands. The following are some possibilities in order of decreasing technology maturity: quantum accelerometers; quantum electromagnetic sensors; quantum inertial sensors and quantum gyroscope; quantum magnetometers; quantum gravity sensors; quantum entangled sensor networks; and quantum radar. These quantum sensors could have a wide variety of applications. Their non-quantum incarnations are widely used in personal, industrial, medical, and military applications. Quantum sensors will be attractive where the precision and sensitivity in a narrowly targeted band is important. They could also provide low SWaP and stability in industrial and military settings. Given their newness and specific properties, the creativity of scientists and engineers will take us beyond the applications of the current sensors. Already medical and scientific devices have started using simple Quantum sensing. For the DoD, the unique applications could be in Intelligence, Surveillance, and Reconnaissance (ISR), PNT (especially, navigation by alternative means), and communication.

All sensors are subject to spoofing attacks and most are subject to corruption of information between sensors and user applications. New cyber and/or Cyber-EW attacks and consequences may depend on specific sensor type. Narrower signal range may help mitigate some risks while sensitivity and precision may create new lower-level vulnerabilities. Possible new side channel attacks could surface in quantum sensor systems.

The following are S&T goals motivated by the above discussion. Note that one attack mode and one solution may not fit all sensors so the following may have to be repeated to cover important sensor types.

a. Identification of attack modes on quantum sensors and mechanisms for prevention
b. System designs with built-in resilience against any compromise of sensor or eco-system
c. Effective cyber-EW attacks on new quantum sensors

3.12.3 Computing

Clever use of superposition and entanglement properties allow parallel operations on qubits, thus changing, compared to the classical computers, the basic complexity level for several classes of problems and algorithms. As the qubit and quantum volume (QV) capacity of quantum computers (QC) improve, QC may surpass the ability of classical computers for these classes of problems and the difference will grow exponentially beyond this crossover.

Bounded-error Probabilistic Polynomial time (BPP) is defined as the set of problems solvable in polynomial time by classical computers and Bounded-error Quantum Polynomial time (BQP) is the set of problems solvable in polynomial time with high probability by QC. Then, any applications that benefit from addressing problems in BQP that are not in BPP will benefit from the use of QC when they reach large enough qubit/QV capabilities. Since discovery of new algorithms leveraging QC may change the problem classification, it is not possible to list all problems in BQP that are not in BPP. However, several important problems are in BQP and there are no known classical algorithms to put them in BPP. One important class is associated with the currently used asymmetric encryption (Integer factorization and discrete logarithms) in public key infrastructure (PKI). Thus, a QC with large enough qubits and QV capacities can break encryption used in most of the deployed DoD systems and in most commercial systems. That fact is a big driver for investment in technologies to build QCs with larger capacities. Simulation of many physics phenomena have also been shown to be in BQP. Other problems may see their complexity change significantly with QC even when the speed up is not exponential. Finally, new quantum algorithms for many important problems may provide exponential speedup and move these problems to BQP. Expectations are that QCs will address several problems in biology, physics, neuroscience, and medicine development that are beyond the reach of classical computers. Another possible application of QC may be in cryptographic computing.

Current QC capabilities are far from the crossover point from classical computers for any important known algorithm in BQP that are not in BPP. However, some projections suggest that the qubit capability will go from 127 in 2021 to over a million in 2030. If it continues to grow at that rate, it is possible that the crossover could happen within 15 to 25 years for the current asymmetric encryption used ubiquitously and the entire PKI could be affected. Given the time it takes to standardize Quantum Resistant Encryption (QRE) algorithms and protocols, develop infrastructure, and replace all current implementations, it is important to standardize QRE algorithms and protocols as soon as possible. For other high-impact applications of QC, it is perhaps too soon to be devoting significant applied research and technology development effort.

The following S&T goals are motivated by the discussion above.

a. Development and standardization of QRE algorithms and protocols

b. Cyber defense for new computing architecture for QC and its interface with classical computing and communication systems
c. Quantum algorithms that may help scale HE, SMPC, PPS, and new quantum ML algorithms for cyber defense and offense

3.12.4 Communications and Networking

One obvious application of quantum science for communication is new techniques to protect data in transit. Two quantum properties investigated to achieve this goal are entanglement and state collapse.

While a qubit can exist in probabilistic superposition of two states (0 and 1), any observation of the qubit collapses the state to 0 or 1. Thus, any eavesdropping on communication using qubits will be detected easily. This property could be used to carry out secure Quantum Key Distribution (QKD) that is followed by classical communication using the selected keys. QKD is a mature technology and is deployed in several terrestrial trial networks and over some satellite links. In 2017, the first intercontinental video conference using quantum encryption took place between the presidents of the Austrian and Chinese academies of science. The cryptographic key pair used by the stations in Vienna and Beijing had been generated using an optical QKD payload aboard a Chinese satellite in orbit since 2016. QKD adoption since then continues to grow in certain networks, currently linking four areas - Beijing, Jinan, Hefei, and Shanghai, referred to as Quantum Metropolitan Area Networks.

However, QKD suffers from easy denial of service (DOS) attacks and several other deficiencies, and is deemed unsuitable for serious applications.

Another approach for using quantum properties for secure communication is called teleportation. A source sends entangled photons to transmitter and receiver. The transmitter allows the photon to interact with qubit and transmits the result to the receiver. The receiver can use that information to figure out what the transmitter was trying to transmit. The technique could be used for just the key exchange or for all transmissions. This approach is at an early research stage.

There are several other promising research results for the applications of quantum physics to communication networks. One is to reduce the impact of noise in communication line. Another is to use more than two state to harden entanglements.

Quantum Random Number Generators (QRNGs) provide streams of random numbers with better entropy than their classical counterparts and they are based on well understood and easily verifiable physical properties. Many new devices are equipped with QRNGs. A commercially available quantum random number generator, the Quantis QRNG SoC developed by ID Quantique, first appeared in a commercial Samsung phone in 2020. QRNG processors will continue being embedded in consumer products such as IoT devices, mobile phones, automobiles, and infrastructure. Hardware based QRNG products or services are currently available from ID Quantique (Geneva, Switzerland), Quintessence Labs (Canberra Australia), and Picoquant (Berlin, Germany). Microsoft offers a software based QRNG with development kit.

3.13 Cyber-Physical Systems

$1.8T Weapons systems face two top challenges, SW and Cyber (GAO June 2020)

Our reliance on computing to supervise, monitor, and control key pieces of critical infrastructure combined with the mass expansion of commodity computing create a massive attack surface. Our current attempts to defend these resources do not account for the sophistication of an adversary committed to damaging US interests- Raytheon CODEX

Cyber Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and cyberspace logic. CPS bring advances in transportation and logistics, manufacturing, electrical grids, health care, emergency response, and almost all critical infrastructures. They include a whole range of physical systems that have been increasingly cyberized over the last two decades. Examples for the DoD include ground, air, space, and sea based military platforms used for logistics and warfighting, weapons systems, micro-grids, robots, and delivery of medical help. Many platforms and swarms of these platforms are getting semi-autonomous in mobility and decision making, and could become autonomous in the future. Tightly coupled physical and cyber aspects of CPS create new challenges for cyber but also offer some advantages compared to general purpose computing (IT): Sensors in multiple domains; clearer mission context; physics and models of physical systems to guide the trade-offs and controls. Despite significant attention over the last decade, many challenges and opportunities have not been explored adequately, especially those involving cyber and physical aspects together. Commercial and defense industries have realized the importance of bringing cyber and physical systems expertise together to address these challenges and opportunities fully. The following S&T goals are motivated by these observations.

a. S&T at the intersections of cyber and physical (also including human aspects where appropriate) addressing the following.

Very difficult to defend against, both technically, and because of lack of communication between cyber and physical research groups. "A Digital Pearl Harbor is waiting to happen". Needs a paradigm shift on how they think about their systems. –B. Miller, Penn State ARL

- Identification of areas of strong interconnections and development of integrated semantics
- Integrated vulnerability analysis. Joint 'fuzzing'
- Integrated system models
- Joint designs of sensors and sensor networks to enable more effective anomaly detection
- Joint analytics and integrated control actions

Note that there are major differences among physical domains in different types of CPS and each type will need its own customization.

b. Binary analysis of the code in Supervisory Control and Data Acquisition (SCADA) and Industrial Control systems (ICS). SCADA and ICS are key situation awareness and control tools for many CPS. Increasingly, they reuse code from common code libraries. This creates a significant threat landscape that should be tracked. Binary code analysis to look for malicious content in binary executables is critical.

c. Autonomic resilience techniques that achieve optimal operating points while trading off among confidentiality, integrity, availability, and control. Given significant differences between OT (CPS) and IT in mission context and physics, the optimal operating region in the trade-off could also be very different. For example, integrity, control, and availability are likely to be more important than confidentiality during operations of CPS. Also, the trade-offs may change over time after a failure or a compromise. Many well-designed cyber-physical systems can function for a short time without cyber support. Availability may be less important than integrity and control during this period but may become more important with time. It is important to capture these trade-offs in designing autonomic resilience that minimizes mission impact after a compromise.

Many existing techniques from software engineering can be inaccurate and error prone when applied to generic programs. But in the CPS domain, if we take a domain-specific approach and leverage the control model when applying these techniques to the control program, we can get more accurate results. Knowledge about the control model reduces the search space for techniques like fuzzing and debugging.-Professor D. Xu, Purdue University

d. Autonomic resilience based on operating constraints. Mapping mission context and physics to operating constraints and designing anomaly detection and autonomic control actions based on these constraints.
e. Formal and semi-formal verification of the designed security within mission context
f. Use of ML to improve decision making and/or facilitate autonomous operations. Human-ML teaming with increasing control to ML over time. Note that the challenge of trustworthiness of ML increases as the system becomes increasingly more autonomous (reducing the role of HIL).

3.14 Internet of Things (IoT) and Proliferation of Relatively Low Resourced Devices

Some have blurred the distinction between CPS and IoT. In order to identify a very different set of challenges and opportunities, **IoT here is defined as low SWaP devices connected into the network**. Frequently, these devices are sensors in home, businesses, CPS, manufacturing, and other critical infrastructures. Low cost, large quantities, and global connectivity allow these devices to provide accurate situation awareness and carry our commands that translate to simple actions by end devices. Short range and high spectrum reusability in mmWave and THz communications (e.g., 5G/6G) will allow a large density of these devices generating enormous amount of data for situation awareness. However, these low SWaP devices can be compromised relatively easily and provide false data. These connected devices also provide access to wide area network with far richer targets. The following are S&T goals to address new challenges and opportunities. As noted earlier, IoT, Edge computing, and 5G feed on one another and there is some duplication in the S&T goals discussed in sections related to these technologies.

IoT purpose doesn't include cyber, cyber is an afterthought with no room left for it the device-J. Li. Siege Technologies

I worry that the security posture for IoT is broken-Dr. M. Linderman, AFRL

a. Discovery and mitigation/weaponization of vulnerabilities in lightweight communication protocols used in IoT
b. Identification and mitigation/weaponization of vulnerabilities in Operating Systems of low SWaP IoT devices
c. Designing secure software updates to low SWaP devices
d. Designing effective encryption and authentication for IoT devices. Security of 'what you have' in multi-factor authentication of IoT devices; restrictions imposed by low SWaP; Quantum Resistant Encryptions that can be accommodated in IoT devices.
e. Reduced-burden cyber defense
f. Architecture solutions to IoT security
   I. Redundancy and diversity
   II. Self-monitoring by IoT cooperative
   III. Ability to function securely even if a fraction of devices is compromised (Byzantine fault/compromise tolerance). Trust model that allows obtaining reliable data from a mix of untrustworthy, neutral, and compromised devices.
   IV. Gateways with additional two-way access controls and data protection

3.15 ‘Realistic’ Digital Persona and Deceptive Digital Content (DDC)

Digital persona can be described as “the model of the individual established through collection, storage, and analysis of data” about a person. These digital personas have many applications. Following are some examples: User profiling and authentication; audience/customer characterization and marketing; virtual teams to brainstorm alternative ideas and help decision making; develop virtual reality world; faking identity; masking the true behavior of a user in the network.

Fake text, images, audios, and videos can be used to initiate and/or promulgate a false narrative that seems true and authentic. These highly realistic deceptive digital content (DDC) could be used to change the perceived reality, trust in news as a source of information, trust between people, between people and Government, and between Governments. Deep Learning techniques can help generate even more realistic DDC.

Over the last five years, there has been an unexpectedly rapid advancement in technologies to develop DDC. Powerful data analytics, image alternation, and sound overlay and alternation, coupled with DL will continue to advance these technologies well beyond the current ‘deepfakes’.

The following are some S&T Goals from cyber perspectives:

a. Advanced user profiling and authentication using digital persona
b. Targeted ‘phishing’ attacks using advanced DDC
c. Techniques and analytics for detecting fake digital persona
d. Technologies for detecting and creating DDC
e. Cyber defense through advanced DDC
f. Digital persona for simulating cyber-attack/defense battles to develop strategies and tactics.
g. Information and Influence Operations using advanced DDC

Cyber deception agents will be like firewalls of today- Professor E. Al Shaer, CMU

Shadow world we live in within the real world- Professor E. Professor Al-Shaer, CMU

3.16 Integration of Bio, Neuro, Cyberspace, and Physical

For several decades, there has been research attention to brain-inspired computing and bio-inspired physical systems. Also, human-machine teaming today involves human intelligence working with machine intelligence using machine language. However, direct integration of bio and/or neuro with cyber and physical is recently getting serious attention. The communication between bio-neuro and cyber-physical (organic and inorganic) could start out using machine language, move to natural languages, and eventually to brain waves. A whole new world can be created, changing the way we live and fight, communicate and make joint decisions. The following are some examples of the evolution from here to there: Exoskeletons supporting humans; machines (exoskeletons, computers, vehicles, etc.) controlled by human brain using brain waves for communication; Brain-computer hybrid working as a single entity, possibly via direct brain implants communicating with inorganic computer at cyber speed; Brain to brain communication using brain waves and multiple brains discussing and making important decisions.

Given the potential benefits in personal and professional lives, these technologies with proliferate rapidly when believed to be mature and affordable enough, and nothing will be able to stop them even if the societal and security implications are not fully understood during the initial deployment. In any case, these technologies will create vulnerabilities that will have to be addressed, especially in warfighting context. The following are some of the S&T Goals to be considered.

a. Prevention of any compromise of the brain-machine and brain-brain communication
b. Autonomic resilience. That is, the ability to minimize the mission impact after a compromise. This includes Byzantine attack tolerance.
c. Verification of inorganic devices connected directly to the organic brain and body
d. Prevention of inorganic intelligence taking over the control of organic brain and body
e. Biologically designed cyber regulatory systems to take advantage of evolutionary intelligence built into human body and brain

3.17 Artificial Intelligence (AI) and Machine Learning (ML)

> *"It's a national security issue if China controls the development of AI specific chips"- Dr. J. Alstott, IARPA*

AI evokes vastly different responses even among scientists and engineers. Some believe AI is applied to problems for which you already have a solution; a device with programs containing known solutions. Others believe it will radically change personal and professional lives, commerce, as well as all military conflicts.

Artificial Intelligence (AI) is sometimes defined as the entire universe of computing technology that exhibits anything remotely resembling human intelligence. On the other hand, with more specificity, AI is defined as technology that allows computers and machines to mimic the perception, learning, problem-solving, and decision-making capabilities of the human mind. The former includes many rule-based decision systems, expert systems that capture knowledge and wisdom of experts, and the systems that could learn to perceive, reason, solve new problems, and make decisions like humans do. The latter definition seems to demand much more from AI systems. Many use the former definition and a large fraction of the AI systems in operation today are simple rule-based decision systems or autonomic systems that capture objective models, subjective human expertise, and results of sophisticated analytics run offline and programmed into the systems to provide human like responses in real time.

One modern taxonomy defines three stages of AI:

- **Artificial Narrow Intelligence (ANI).** ANI can carry out a single, specific, and narrow task very well, but may fail in addressing other tasks, cognition or understanding. ANI is not socially aware or conscious, placing it below human brain and far below the capabilities of super-intelligent AI. Despite these limitations, ANI has succeeded in many applications and provided dramatic results. Most AI successes to date have been for ANI.
- **Artificial General Intelligence (AGI):** AGI is the hypothetical ability of an intelligent system to understand or learn any intellectual task that a human being can. Cognition and reasoning are important aspects. Some require sentience and self-awareness. True AGI may be 2-4 decades away but interim AI technologies could be powerful enough for serious applications beyond ANI.
- **Artificial Super Intelligence (ASI);** ASI is AI that evolves to become self-improving and can eventually surpass human intelligence and technological advancement. This type of AI is often referred to as "Technological Singularity" or "Superintelligence".

ML is the use of computational methods and algorithms to "learn" information directly from data without relying on a pre-determined model. ML technologies have become the most important set of tools for AI in recent times and is the focus of attention in this study. As ML techniques move from specific tasks to general tasks and broader learning, AI will move from ANI to AGI.

After decades of slow progress, ML has seen phenomenal acceptance in a variety of applications. In addition to innovations in methodology, the computing power afforded by GPUs allowed DNNs and DRL to be employed on large datasets. A wide range of pattern recognition and classification applications has benefitted. For examples: Image recognition, anomaly detection, NLP, and DNA analysis. Technology companies, social media platforms, and marketing companies have used ML to develop recommender systems that convince us what to buy, who to vote for, what to believe, and what decision to make. ML has also been used to tell vendors how to segment the market and what to market for each segment. ML is playing and likely to play a large role in robotics and autonomous platforms. Research papers in many fields now include some ML for their domain. Recently, NSF saw that 85% of proposals in control theory included some form of ML. Some experts claim that loss of leadership in this area will create dramatic shift in economic and military leadership on the global stage.

While ML (and AI) has become a 'must have' by all, the actual successes of ML techniques is still limited to a small number of problem types, relatively benign environment, and error tolerant applications. The combination of high accuracy, adversary tolerance, and ubiquitous applicability is far from having been realized.

On one hand, ML is a very influential cyberspace technology. On the other hand, it could improve other cyberspace technologies and systems. ML can also play a significant role in improving cyber defense and offense, but it could bring new cyber risks. These multi-faceted relationships raise the following issues, discussed individually in Sections 3.17.1 through 3.17.5.

- Current and future roles of ML in cyberspace technologies and systems. Analysis of benefits and risks. New cyber vulnerabilities introduced by the use of ML.
- Current and future roles of cyberspace technologies in enhancing ML capabilities and applications. Cyber vulnerabilities and impact on ML applications.
- Current and likely roles of ML in cyber defense and offense and related Information Operations. Related risks and mitigation.
- Trustworthy ML
- Future of S&T in ML

3.17.1 ML in Cyberspace Technologies and Systems

In general, ML helps cyberspace improve decisions and adaptions based on past experiences (in the form of data) and changes in environment. By providing this machine intelligence, ML also helps reduce the need for expert humans in the control and management of cyberspace.

3.17.1.1 Networking, Communication, and Computing

The following are some important examples of networking and computing systems where ML will play important roles.

1. ML for network management. AI, in the expert system form, is already important in modern network design and management, especially in anticipating and reacting to failures. Rapidly growing network infrastructure, user base, and services point to the value of ML in control and management. If concepts like CBN are deployed in future networks, ML could play roles in determining caching locations and movement of data among them, another aspect of management. Domain specific explainable ML and human-ML teaming technologies may be extremely useful for network control and management applications.
2. ML in the core networking and communications functions of cellular wireless networks. Emerging and future wireless access networks (e.g., 5G/6G) are projected to provide increasing degree of programmability and use ML in basic protocols and controls, in addition to management of several new and important features. The amount of data produced from large number of user- and infrastructure-devices will enable statistically meaningful ML for management. On the other hand, core protocols and controls typically operate without human monitors and effectively run the networks. Increasing use of ML at that level will open up the networks to serious adversarial attacks on ML, as discussed in Section ML in managing cloud infrastructure, virtualization, microsegmentation, and microservices. The last three enable tremendous flexibility and speed in developing new services, customizing services, and providing differential security. ML could help with data driven decisions. However, as discussed in Section 3.17.4, possible adversarial attacks on ML will add to the overall cyber vulnerability of these flexible clouds.
3. ML in automated software development, including malware development. DevOps supports some level automated software development from specification. Several software companies and Government labs are in the process of taking advantage of the available and new building blocks as well as tools for integration to reduce human involvement in software development. ML could take this automation farther. The nexus of the concept is that a computing system could take from the human a high-level description of a desired function and produce code that performs the functionality. In this hypothetical scenario, the machine intelligence would have the ability to test, debug, and optimize its own code, perhaps via GML or GAN-style architecture, and could perform this iterative development cycle significantly faster than a human team of software engineers. This is of course a vision for the future. If this system were to exist, the ramifications would be far-reaching, but one area of particular interest to this study would be in the cyber domain, both defensive and offensive. A system which was given the high-level specification of 'gain root access to a target network' could potentially develop extremely dangerous malware- a system that could learn and adapt to updated network defenses on the fly, could spread beyond its original concept of operations, and cause damage far beyond its original intent.

4. ML in automated designs of protocols and systems. Automated protocol and system architecture designs are more complicated than software development. However, ML could improve the accuracy and speed of NLP, designing building blocks, selecting the right building blocks, and integrating them based on high level specifications. These could speed up the automation. Once again, the concerns expressed above for software apply here.

3.17.1.2 Cyber Physical Systems (CPS) and IoT

1. CPS are important areas of application of ML because of important data driven decisions to be made in these systems. The CPS with some degree of mobility (cars, drones, military platforms, weapons systems, etc.) are even more important because mobility itself can benefit from ML. Thus, ML could have impact on personal and commercial transportation, product deliveries, supply chains to the battlefield, as well as the whole battlefield. Previously dumb platforms could become smart and possibly autonomous, keeping humans away from danger, and breaching anti-access barriers. However, CPS are vulnerable to cyber-attacks with devastating consequences. ML could help address the vulnerabilities and enable adaptive cyber defense but, as discussed in Sections 3.17.3 and 3.17.4, will also add more attack vectors.
2. Low SWaP IoT devices will start dominating the number of connected users and serve many personal, commercial, and industrial needs. Some devices may not be able to support full-fledged ML systems. However, a network of ML capable software agents spread over many devices and servers could provide more effective support to the mission. Cyber-attacks could affect the integrity of the sensor data, command and control, and the mission. On the other hand, low SWaP-C IoT devices with ML overlay may allow self-monitoring and Byzantine attack tolerance.

In the applications discussed in Sections 3.17.1.1 and 3.17.1.2, ML is meant to improve the performance of the cyberspace systems while also reducing the need for expert humans to run the systems. However, as discussed in Sections 3.17.3 and 3.17.4, the data and algorithms used by ML are vulnerable to cyber-attacks and adversarial manipulation. The result could be loss of critical information, loss of service, performance degradation, loss of control, and even serious damage to properties and loss of life.

The above discussion motivates the following S&T goals for the use of ML in networking, communications, computing, CPS and IoT:

a. Effective human-ML teaming to support control and management of spectrum, network infrastructure protocols, and services. Domain specific and explainable ML could help. Also important are technologies and interfaces for human ML teaming designed to facilitate migration to decreasing roles of HIL.
b. Effective human-ML teaming in automated software and protocol development, and formal verification. Domain specific and explainable ML could help.
c. Use of the mission context to evaluate the risk-reward trade-off for every major step towards ML and autonomy
d. ML in the analysis of data from sensors in cyber and physical domains of CPS. Identification of anomalies and constraint violations. Domain specific and explainable ML could help relate anomalies to cyber-attacks or other forms of adversarial manipulations.
e. Representing constraints on the CPS behavior and their use in controlling the consequences of errant or corrupted ML
f. Design of IoT network architecture. Roles of ML in individual devices and centralized servers. Control of the spread of an ML compromise. Ability to process and disseminate valid information despite any compromise.

3.17.2 Cyberspace Technologies in Support of ML

ML relies on other cyberspace technologies in many ways.

a. High speed computing. Most ML, especially Deep Learning (DL) techniques such as Deep Neural Networks (DNNs) and Deep Reinforcement Learning (DRL), rely heavily on high-speed computing. In fact, the advent of GPU enabled scalable DNNs and DRL resulted in noticeable successes over the last decade.
   - Tensor Processing Units (TPUs) will offer even higher computing speeds and enable further scalability for ML
   - In the far term future, quantum ML algorithms running on QC could provide exponential speed up compared to classical algorithms on classical computers
   - Ever increasing storage capacity allows massive amount of data in one place for ML algorithms to train on
   - Cloud computing will allow an average user to have access to high-speed secure computing for ML applications, and even ML as a Service (MLaaS) from cloud service provider, thus democratizing ML
   - Advances in microelectronics allow heterogeneous chips with multiple chiplets and, in particular, enable ML capabilities in a chip. The chip could also include other components such as CPU, GPU, and ASIC. Such chips provide tremendous gain in the performance and scalability of ML algorithms.

b. High speed networking. This facilitates movement of large amount of data in a short time, thus enabling the ML training and test data from multiple locations to be brought together analysis. On the other hand, Edge computing advances allow distributed ML calculations without moving all data to a centralized location.

Note that the cyberspace technologies and systems supporting ML applications are vulnerable to cyber-attacks, thus jeopardizing the ML applications themselves. More about this is presented in Section 3.17.4.

3.17.3 ML in Cyber Defense and Offense

Cyber and ML have a two-way relationship. Machine learning (ML) could be an important enabler of scalable defensive and offensive capabilities in cyber battleground. The proposed applications range from semi-automated decision-support tools to fully automated capabilities. However, ML models for most applications can be exploited in at least four ways: 1) attackers can poison the data used to train ML algorithms to degrade prediction quality or redirect predictions altogether, 2) attackers can evade by manipulating runtime data to ensure ML models misclassify malicious behavior as benign, 3) attackers can infer information about training data, and 4) attackers can approximately reconstruct the ML model for further analysis and exploitation. These adversarial manipulations could have serious consequences and it is important to develop Trustworthy ML that could provide resistance and resilience to these attacks. The ML applications for cyber defense and offense are discussed here. Trustworthy ML is discussed in Section 3.17.4.

The following are some examples of potential applications of ML for Cyber Defense and Offense:

a. Automation in the following steps of managing cyber vulnerabilities in architecture, protocols, software, and firmware
   i. Discovery
   ii. Analysis for exploitability
   iii. Mitigation, self-correction, and verification
   iv. Design and characterization of cyber weapons

Common ML approaches using large historical datasets to train the model may not always be suitable for the above. Integration of static and dynamic program analysis, testing/fuzzing, and ML (particularly, GML) seems very promising.

b. Automation of the orchestration of many capabilities provided in the system to maximize mission success even after the cyber system is compromised by the adversary. The use of ML in orchestration allows adaptation based on historical data or results of game playing ML techniques, thus moving from autonomic to autonomous.

Cyber SA and Cyber C2. As discussed earlier in Section 3.4.5, Cyber SA and Cyber C2 use analytics to help humans build situation awareness from the sensor data and to evaluate alternative cyber maneuvers for defense and offense. In this report, it is assumed that Cyber SA and Cyber C2 as human-managed functions, and ML could help humans respond faster and more accurately. ML technologies also support humans in learning from past performance and thus allowing adaptive defense and offense. Over time, some aspects may move to autonomous adaptive defense/offense.

c. The following are some examples of functions where ML technologies could help develop Cyber SA:
   - Sensor information fusion
   - Intrusion detection, (obfuscated) signature detection, and anomaly detection
   - Adversary characterization
   - Malware analysis
   - Attribution
   - Tracking adversary movement in cyberspace
   - Battle Damage Assessment (BDA)

d. The following are some examples of functions where ML analytics could benefit Cyber C2:
   - Assessment of mission impact
   - Evaluating traditional cyber maneuvers such as deception, evasion, stealth, morphing, as well as the use of DCC
   - Assessing likely consequences of an action, especially activating a cyber weapon
   - Finding the 'best' action
   - Use of GML and GAN for assisting actions described in the above three bullets

Note that most items in 'c' and 'd' above could be and are executed without the use of ML. ML enables learning from data to adapt interpretation and actions, thus enabling adaptive cyber defense/offense. It should also be noted that ML does not equate to autonomy, but it could facilitate autonomy by replacing the use of human intelligence with machine intelligence, where appropriate. Thus, all of the above will involve human-ML teaming and could reduce human involvement over time. Also, for 'c' and 'd', ML models could be trained offline and fed to the system to take actions based on 'test data' collected from sensors and observations. This approach could be useful during earlier stages as well as when the real system (like a low SWaP IoT device) does not have the capacity to run ML training. It could also be useful when historical data from multiple devices are needed to train the model. An extension of this approach could involve enhancing the model trained offline by incremental online learning.

The following two are broader uses of ML for helping several Cyber defense/offense techniques.

e. ML for Natural Language Processing in support of several of the above. In particular, for mapping textual specifications to formal requirements and mapping textually specified intent to formal requirements.

f. Cyber warfare/battle simulation using ML based agents.

All of the above could benefit by combining human expertise, statistical machine learning, and formal domain information.

As mentioned in Section 3.17.3, adversarial manipulations of the ML processes, data, and algorithms could lead to serious consequences for the mission of the system supported by ML. In addition, the system users and operators could lose trust in ML and even in the system itself. These lead to two general sets of S&T areas: Trustworthy ML and Cyber Attacks on ML.

3.17.4 Trustworthy ML: Preventing and Countering Adversarial Manipulations

Trustworthiness of ML has become important enough and generated enough interest to warrant an entire taxonomy by NIST. At a high level, Trustworthy ML includes security, reliability, explainability, fairness, privacy, and governance. From cyber S&T perspective, security and privacy play major roles, while explainability could make it harder to hide adversarial manipulations and boost trust in ML. The focus of security and privacy aspects in the current context relates to resistance and resilience to cyber-attacks that could otherwise adversely affect ML processes, data, and algorithms and hence the mission of the system supported by ML.

Attacks on ML could be at training phase or at testing/evaluating phase. Much has been written about types of these attacks and countermeasures in the context of computer vision applications. Given that cyber terrain is quite different from computer vision, it is important to understand and address critical challenges and opportunities in the context of cyber. Sections 3.17.1 through 3.17.3 list three types of ML applications that are vulnerable to such attacks.

1. ML supporting cyberspace technologies and systems: A successful attack could impact the mission of the system or service supported by the cyberspace technologies. Examples of systems: Network supporting C4I, manufacturing supported by IoT, and a military platform supporting kinetic battles.
2. Cyberspace technologies supporting ML. The attack could start in the supporting cyberspace technology such as microelectronics and cloud services. Successful attack will impact the mission of the system or service supported by ML.
3. ML supporting cyber defense and offense. Successful attack on ML could deceive and defeat the cyber defenses, mislead reconnaissance, and mislead offensive cyber weapons. Note that cyber is inherently adversarial and ML could be manipulated by adversary, thus creating a unique situation when they are coexisting. It is conceivable to have defensive and offensive software agents supported by ML fight cyber battle against each other without human involvement.

Some important challenges and opportunities to be addressed by Cyber S&T for Trustworthy ML include:

a. Direct and indirect poisoning of training data: prevention and resilience
b. Poisoning of test data: prevention and resilience
c. ML logic corruption: prevention and resilience
d. Countering evasion
e. Oracle based attacks: prevention and resilience.
f. Tools to discover and characterize vulnerabilities in ML.
g. Formal verification of trustworthiness of the ML in the mission context
h. System level security in the context of complex cloud-based ML applications.
i. Use of adversary CONOPs in ‘a’ through ‘e’ above in developing techniques to prevent those attacks

Trustworthy ML: Suitability for Critical DoD Applications

The above discussion of Trustworthy ML related to preventing and countering adversarial manipulations of ML data, algorithms, and process. There is another important aspect of trustworthiness: Accuracy of results vs requirements and expectations. Practical use of ML for any application requires certain accuracy in results/recommendations for the user to see enough benefits and develop trust in the technology. The threshold depends strongly on the application, CONOPs, and degree of autonomy given to the ML. For example, when applied to detection (malicious, dangerous, enemy vehicle), the accuracy translates to false positives (e.g., declaring benign as suspicious) and false negatives (not declaring malicious as malicious). Most ML techniques allow some tradeoff between false positives and false negatives for a given amount of data. If the tradeoff curve is way outside acceptable region for the application, user, and CONOPs, the technique will not be trustworthy to the user and acceptance will be difficult. Similar considerations apply to other applications of ML technologies.

It is conceivable that techniques found successful in some commercial applications may not be suitable for other commercial applications or DoD applications. It is important to have the tools to determine suitability. Thus, the following S&T goals are relevant.

j. Quantitative methods to understand the tradeoff curves for ML techniques of interest and the acceptable region for the application and user population.
k. Quantitative methods to evaluate the impact of the adversarial manipulations on the trade-off curve and improvement achievable by a mitigation technique.

3.17.5 Ongoing and Future Challenges and Opportunities for ML: Relationships with Cyber S&T

Items in a-f in Section 3.17.1, a-f in Section 3.17.3, and a-k in Section 3.17.4 are all important S&T topics in near, mid and far term future. Several of these topics have seen significant basic and applied research but more needs to be accomplished. While most S&T items in those sections are described from cyber defense perspective, they obviously apply to the cyber offense. Given the expected prevalence of ML in all conflicts, S&T for the offensive counterparts is especially important.

Some additional S&T goals and detail are presented below.

a. Domain specific ML. ML techniques that combine formal domain knowledge with statistical ML
b. S&T for challenges and opportunities at the intersection of cyber and ML
c. S&T at the intersection of cyber, ML, and domain of application of ML
d. Explainable ML. This is important for human-ML interactions, building trust in ML, and identifying anomalies in the results from ML algorithms. Ideally, human should be able to look at the results and explanations, ask 'what if' questions, and get answers. However, the user could be an ML expert, a cyber-expert, or an expert in the domain of application of ML (if it is not cyber defense or offense). Explainability for each should be available. Overall, this is a huge S&T challenge. Domain specific ML could make it easier to achieve better explainability.
e. Technologies supporting effective Human-ML Teaming. This is part of the general human-machine teaming effectiveness. The explainability discussed above will help the teaming. However, effective teaming will also allow humans to teach ML and ML to teach humans. Combination of domain models, human expertise, and statistical techniques could improve results and speed of decision making. In addition, it will permit a natural transition from ML supporting human, to human supporting ML, to human on the loop monitoring the ML performance, and tweaking parameters when needed.
f. Use of software agents with ML capabilities to provide autonomous cyber defense and offense. Some interesting results are already obtained but more needs to be done.
g. GML and GAN. These are important areas for exploration. Computerized game playing between two entities is used to generate data that can be analyzed in developing strategies. Since cyber is inherently adversarial, the approach using defensive and offensive software agents with ML capabilities to play attack-defense battle could provide valuable insight as well as data. RL and DRL could play significant roles, along with GML and GAN. Among the novel cyber defense and offense technologies possible using this approach are the traditional cyber deceptions as well as the media based DCC.
h. Use of increasing computing speeds from TPU, custom processors, and custom ML chips. The increasing speed, coupled with improved techniques such as scalable DNN, DRL, GML, and GAN could continually expand the problems that can be solved, decrease the training time, and expand the set of devices on which a trained model could run on.
i. New models that can be trained once and deliver (via fine tuning or minimal additional learning effort) solutions to many problems, thus enabling the use of ML where the available data is sparse, but a model trained on another type of data can be repurposed. Depending on the relationships between the original problem and new problems, this approach could be considered incremental learning or transfer learning.
j. Control of the effect of cyber weapons created by ML autonomously. Without appropriate controls, it is possible to develop a cyber-weapon that behaves like a living bioweapon. It could spread and mutate and learn. This will both increase the amount of damage that it can cause, and significantly increase the potential for unintended consequences. It could result in a really risky window where the technology is dangerous, but the institutions are not culturally prepared to handle it (i.e., a research experiment goes wrong, and massive damage occurs).
k. Techniques that work with small datasets. One example is incremental learning. Others involve transfer learning or the use of domain models to reduce the size of dataset required.
l. ML models which employ concepts based on biological brain. These could use silicon-based processing architecture in the near future (neuro-inspired computing) but move to biological computers that could bring ML closer to AGI.

m. Influence of culture and governance structure on the types of ML capabilities developed and employed. Different nations and non-nation actors will not use the ML similarly. These differences are critical for commerce as well as in military conflicts.

3.18 Rapid changes in Cyberspace Technologies: Need for Tools and Platforms (Analytic, Simulation, and Emulation)

Core cyberspace technologies are changing rapidly and increasing programmability allows creation of significantly different versions on the fly. Rapid analytics are needed to evaluate the impact of these fast changes on the cyber battleground. Many interactions between cyberspace and cyber defense/offense are too complex to easily reason, draw inferences, and develop action plans without significant machine assistance. Building new models from scratch is a time and resource consuming endeavor and not effective in a shrinking timeline environment. It is important to develop platforms and analytic tools to put together new models quickly. A repository of analytic modules and standardized data formats are critical for the speed of development of new models. Commercially available modules provide a good starting point to build domain specific libraries.

In many cases, the complexity prohibits tractable mathematics to quantify the interactions and identify optimal actions in each possible state. However, modern day computing power allows scalable computer simulation and emulation models to help evaluate the interactions and develop optimal action plans. The following are S&T goals for such simulation/emulation activities:

a. Computer simulation platform with library modules suitable for capturing key characteristics of the cyberspace of interest and cyber defense or offense to be evaluated. Ongoing enhancements based on anticipated new cyberspace technologies.
b. Computer simulation models that capture cyber defense and offense working simultaneously as adversaries within the systems
c. Ability to tailor the operating point on the scalability vs fidelity trade-off curve
d. Computer simulation models that can work in real time as the Digital Twin (or mirror) of the real system and recommend actions based on the observed states
e. Computer simulation platforms that facilitate insertion of software agents in simulation models

3.19 Increasing Roles of Cyberspace Technologies in Personal and Professional Lives as well as in Military Conflicts: Perimeter-less Military Conflicts

Due to a combination of massive data collection and analysis by commercial enterprises, self-reporting on social media, and large-scale information compromises from cyber-attacks, it is hard to keep professional lives separate from personal lives. For the DoD, this implies that military conflicts do not have perimeters. Knowledge about personal life of every warfighter and his/her family, their health situations, and other vulnerabilities are games during military conflict. These threats may not have strong S&T connections other than via technologies to create enough noise in the digital persona that collected information is not useful to adversaries. In any case, the implications are serious and should have roles in policies and agreements.

3.20 Summary of Trends and S&T Goals

The table below summarizes the discussion on technology related trends, and, for each trend, the S&T goals motivated by that trend.

Table 3.20-1

Class	Trend	S&T Goals
Broad	Increasing Complexity and bloat in software, protocols, and systems	• *Debloating and defeaturing existing software and protocols* • *Minimalism in future systems. Small, verified modules and Dynamic Composability* • *Techniques for quick verification*
Broad	Ubiquitous programmability. Third-party everything. Reusable code libraries and open source code. Legacy systems. Note: Recent successes in binary reverse engineering could act as a Class C technology fueling automated vulnerability analysis, mitigation, and verification without access to the source code.	• *Increasing automation in binary reverse engineering, vulnerability analysis, mitigation, and verification* • *Rapid and late-stage analytics and verification of implemented system*
Broad	Hyper-automation and shrinking OODA Loops at all levels of cyber conflict	• *(Semi)- Formal methods for SW, protocols, and systems* • *Automated discovery, analysis, and mitigation of vulnerabilities in SW (including binaries), protocols, and system* • *Redundancy, and spatial/temporal diversity (SDD and MTD) for autonomic resistance and resilience to cyber-attacks* • *Autonomic and autonomous triage, cyber- maneuvers, and recovery to minimize mission impact if system is compromised.* • *Natural Language Processing (NLP)* • *Autonomic and autonomous offensive maneuvers*
Broad	Increasingly untrustworthy cyberspace ecosystem. Location and ownership do not equate to trustworthiness	• *Zero Trust strategy and architecture* • *Additional internal encryptions, authentication, and authorization. Between services and between systems.* • *Self-protection against cyber-attacks by data objects*
Broad	Increasing diversity in domains of applications of cyberspace and tighter interconnections with other technologies	• *S&T at the interactions of cyber with other cyberspace technologies and with application domains: ML, microelectronics, applications to IoT, cyber-physical systems, and bio-neuro-physical systems.* • *Bringing mission context in all aspects cyber defense and offense*
Broad	Increasingly multi-domain operations	• *Joint Cyber-EW offense and defense* • *Joint Cyber-EW-Kinetic defense and offense* • *Cyber-Physical and Cyber-EW-Physical* • *Cyber-ML-X*
A, B	Microelectronics: 'Death' of Moore's Law and Dennard Scaling; heterogeneity; multi-source chiplets in a chip; 2.5D and 3D chips; Increasing roles of FPGA; increasing programmability; Loss of 'ISA' as a true abstraction layer.	• *Verification of heterogeneous chips* • *Verification of 2.5D/3D chips* • *Defense against cyber-attacks during FPGA (re-)programming* • *Joint HW-SW verification* • *Design obfuscation by innovative designs and sourcing* • *Self-monitoring chips using trusted chiplet and SW* • *Controlling side channel attacks*
A	Networking and Communication for wireless access (5G/6G, tactical wireless for the DoD) : Heavy reliance on Software Defined Networking (SDN) Network Function Virtualization (NFV); High degree of programmability and dynamics; Uncertain future of the DoD tactical networks	• *SDN: Cyber defense using advantages of centralization* • *SDN controller network architecture for high availability and integrity.* • *NFV: Innovative cyber resistance and resilience using spatial and time diversity, and dynamics (SDD and MTD defenses)* • *Cyber resistance and resilience in presence of complex service offerings, user programmability, and network slicing*

		• *Advanced analytics and simulation on protocols for proactive identification and mitigation/weaponization of vulnerabilities* • *Proactive analytics on to be specified DoD tactical wireless networks of the future and on future adversary networks* • *Intelligent SW agents for control, management, and cyber maneuvers*
A	Networking Backbone: Possible Internet Balkanization: Content Based Networking (CDN); More SDN and NFV; Decreasing visibility of network traffic.	• *If CDN is seriously considered for deployment* o *Autonomic cyber defense* o *Zero Trust architecture* • *SDN, NFV, and ML challenges similar to those for wireless access networks* • *ISR and cyber offense for Balkanized Internet* • *Monitoring increasingly obfuscated traffic*
A, B	Core Computing: Tensor Processing Units (TPU); FPGA based accelerators and custom chips (e.g., ML); Custom processors; Virtualization and separation kernels; Affordable heterogeneity and dynamics	• *Scaling and automation of algorithms for cyber vulnerability discovery, mitigation, and weaponization, leading to full automation of the entire process* • *Use of virtualization, heterogeneity, and dynamics to provide SDD and MTD* • *Techniques for rapid verification of customized and/or reprogrammed versions of SW and HW; delta verification*
A, B	Cloud Computing: Democratization of high-end secure computing; virtualization, microsegmentation, and microservices; Anything as service; Complex supply chain for software.	• *Addressing challenges for cyber offense resulting from democratization of high-end secure computing* • *SDD and MTD; Use of microsegmentation to tailor defensive cyber to customer, application, and data* • *Late-stage verification of SW; verification of binaries* • *Monitoring the service and application behavior for anomalies* • *Zero Trust strategy and internal controls* • *Scalable cryptographic computing: HE, SMPC, and PPS*
A, B	Quantum	• *Defense of atomic clocks from timing attacks* • *Defending quantum sensors from Cyber-EW attacks* • *Quantum Resistant Encryption (QRE)* • *Exploits on Quantum Key Distribution (QKD)*
A	Cyber-Physical Systems, Including (Semi)-Autonomous Mobile Platforms (CPS)	• *S&T at the intersections of cyber and physical* o *Integrated vulnerability analysis. Joint 'fuzzing'* o *Integrated system models: joint sensor and sensor network designs to enable easier anomaly detection* o *Joint analytics and Integrated control actions* • *Using mission context and physics of physical system to build autonomic resilience: optimal trade-off between control, integrity, availability, and confidentiality; anomaly detection* • *Use of ML to improve decision making and/or facilitate autonomous operations*
A, B	Low Resource Internet of Things (IoT) and Edge Computing	• *Defense of lightweight communication protocols and OS* • *Design of secure SW updates to low SWaP devices* • *Design of secure encryption and authentication for IoT devices* • *Reduced burden cyber defense* • *Architecture solutions to IoT security: redundancies and diversity; self-monitoring by IoT cooperative; Byzantine fault tolerance; Gateways with two-way access controls and data protection* • *Distributed Trust model*
A, B	Digital persona and deceptive digital content (DDC)	• *Data analytics for user profiling and authentication* • *Cyber defense through DDC* • *Technologies for creating and detecting DDC*

A, B	Integration of bio, neuro, cyber, and physical: Exoskeletons supporting humans; Brain controlling machines: Brain-computer hybrid working as a single entity; Brain to brain communication using brain waves and multiple brains discussing and making decisions.	• *Prevention of confidentiality and integrity attacks on brain-machine and brain-brain communication; Resilience against successful compromise of the above* • *Verification of inorganic devices connected directly to the organic brain and body. Byzantine attack tolerance.* • *Prevention of inorganic intelligence taking over the control of organic brain and body.* • *Biologically designed cyber regulatory systems to take advantage of evolutionary intelligence built into human body and brain*
A	Space Platforms	• *Secure updates* • *Security against cyber-EW attacks*
A, B	Rapid introduction of new system architectures and protocols with increasing complexity: Need for rapid evaluation and correction, if needed	• *Platform and libraries of modules that can be used to build new simulation models rapidly* • *Flexibility to trade-off scalability and fidelity* • *Simulation of cyber battle between offense and defense* • *Scalable and responsive Digital Twin* • *Intelligent SW agents in the simulation/emulation*
A, B, C	ML: Important interrelationships between cyberspace technologies, ML, and cyber: ML helping cyberspace technologies and systems; Cyberspace technologies helping ML; ML enabling new techniques for cyber defense and offense; Adversarial attacks on ML processes and algorithms Note: Recent advances in DL, GML, and GAN could be significant Class C technologies that could fuel future ML development and applications.	• *ML for Improving cyberspace (almost all Class A technologies)* • *Cyberspace technologies supporting ML (almost all Class B technologies).* • *ML for automated development of SW and protocols* • *ML for automated discovery, analyses, and mitigation of cyber vulnerabilities* • *ML for decision support for cyber defense and offense.* • *Autonomous agents with ML capabilities.* • *Adversarial ML and Trustworthiness of ML in all of the above* • *Characterization of performance trade-offs and acceptable performance region for ML techniques of interest* • *Tools to discover and characterize cyber vulnerabilities in ML* • *Formal verification of the ML in the mission context* • *Controlling consequences of ML generated cyber-weapons* • *Explainability using ML, cyber, and domain semantics* • *Generative ML (GML) and Generating Adversarial Networks (GAN)* • *Domain knowledge in ML* • *ML on small datasets, incremental ML, transfer learning* • *S&T at the intersection of cyber, ML, and domain of applications*
C	Formal Methods Note: These are also S&T Goals since much needs to be done to realize the potential for cyber.	• *Formal verification of implemented protocols, SW, HW, and systems* • *Building block approach could enable scaling* • *Useful specifications*

4 Key Non-Technological Trends That Could Generate New Challenges and Opportunities for Cyber

The focus of the study was on technology and technology related trends that could have a strong influence on the cyber battleground. However, some other trends are worth mentioning here. These were not investigated in detail, but each could have a strong influence on the cyber battleground, types of adversaries, and constraints imposed on the use of technologies.

Warfighting Trends

- After many years of fighting the Global War on Terrors and focusing on violent extremist organizations (VEOs), the attention is being shifted to regional conflicts with strong nation state adversaries in proxy wars. They bring peer level capabilities and conflicts with multiple warfighting domains. Some nations may have decided to invest more into cyber capabilities as a lower cost counter to the tremendous advantages the USA has in the kinetic warfighting domain. Collectively, these new changes in the characteristics of key adversaries pose different types of challenges for the USA in future cyber warfare.

Doctrines

- Joint Staff and Services are increasingly emphasizing all-domain operations. The shift from VEOs to nation state adversaries makes joint operations in multiple warfighting domains even more important. Cyber and EW are natural non-kinetic partners and should be coordinated together in the future S&T. Additionally, it is important to mature integration of cyber, EW, physical, and kinetic (land, sea, air, and space) for future conflicts.

International Agreements

- While there are no separate treaties and International Laws established yet for cyber warfare, it is possible to understand the implications of general warfare laws and treaties for cyber warfare. Those implications put constraints on the allowable cyber offense technologies and conditions under which they can be deployed. For example, some such laws specify restrictions on offensive cyber operations and even on the response to cyber-attack on friendly systems. Two key restrictions include: need for accurate attribution of various roles played in a cyber-attack against the US; proportional response. Thus, in order to direct responses to a cyber-attack, it becomes important to have technologies that can provide detailed attribution for each specific role played in the attack. Required granularity could include malware author, source node and nation from where agents/bots are launched, node and nation from which the attack initiation and C2 are carried out, transition nodes and nations, etc. Similarly, proportionate response requires an accurate estimation of the consequences of any offensive operation.
- Advances in new technologies applied to warfighting have the potential to increase the lethality of the battlefield to the extent that current warfighting strategies are no longer tenable. Advanced UAS, non-kinetic systems such as cyber and EW, and autonomous systems could dominate the future battlefield.

Climate Changes, National and Global Resource Shortages, and Geopolitical Realignments

Climate changes and global warming could change the livable surface on the earth. Water and energy shortages could also change the relative desirability of living in different parts of the world and generate new territorial ambitions. New alliances could result, and Global political map could change dramatically.

These could change relative cyber capabilities of competing alliances. In addition to military conflicts, cyber capabilities will become very important for protecting the energy and water sources and associated smart delivery infrastructure.

On the technology front, semiconductors, batteries, and green energy technologies rely heavily on rare earth metals, which are in limited supply. Semiconductor production relies on high end ultraviolet lithography machines currently sourced by just one Dutch supplier (ASML). The supply chain is very fragile and could result in new geopolitical realignments.

Global Societal Changes

World population is going through counteracting forces. On one hand, advances in networking and computing technologies promise 'cyberspace everywhere' and 'connectivity to everyone who wants it'. The world is shrinking to its cyber-speed diameter. On the other hand, increasing nationalistic tendencies are moving people apart. The difference between 'haves' and 'have nots' is increasing within and between nations. Cyberspace connectivity is playing a major role in exposing these differences. The following could happen as a result.

- Civil unrests within countries could go from bad to worse. People involved will have an easier access to advanced cyberspace technologies and could use cyber weapons as part of the unrest. This is a vastly different adversary to contend with.
- Covert border crossing is likely to increase. Over time, they will get access to cyberspace technologies and cyber weapons that could jeopardize border controls and other forms controls against illegal entries.
- Supply chains for critical technologies could become unreliable.
- Propaganda and misinformation campaigns designed to sway public perception and opinion may increase.

The solutions may involve new technologies as well as understanding of human behavior.

Covid-19 based pandemic has brought fundamental changes in work life. Some could not work because of the type of their work, while others have managed to work at full capacity and pay without the hassles of commuting and many work-related expenses. This has added to the inequities and resentment. As mentioned above, this could lead to civil unrest. On the other hand, the number of 'home warriors' has increased dramatically, and many would continue that way of working even when the pandemic is history. There would then be a desire to provide the ability to perform classified work from home or other locations. Technologies for this 'distributed SCIF' and for dis-incentivizing physical attacks to workers' homes will become important. Other consequences of this trend towards increasing 'home warriors' include migration of population to low cost living areas and rethinking of office space.

Roles of Large Corporations vis-à-vis Nations

Large corporations with expansive access to data have become as powerful as nation states in cyberspace. If they chose to block you, influence you, and feed lies to you, they could, and you could not stop them. They know everything about you without 'spying'. They manage the society. They move across the boundaries of physical nations. They incorporate based on tax structure, immunity against penalties, and other business reasons. In that context, it is not clear what is foreign and what would happen if the enemy were not a country but a corporation, if its business strategy conflicts with the goals of a nation state. The corporations may limit what a country can do to them.

5 Futuristic Projections to Watch

Most of the trends discussed in prior sections could be anticipated with some degree of confidence, and with varying degree of uncertainty in timing. Some advances are easily imaginable but with little confidence in if and when. If such technologies and/or social trends materialize, they could have profound influences on humans, nations, the DoD, and cyber warfare. Thus, while it may be too soon to fret over them, it is important to keep a watch on the progress to identify sudden acceleration and avoid unpleasant surprises. Some of these futures are briefly discussed below.

- Cyber and EW together becoming strong enough to marginalize the ability to use kinetic weapons successfully, creating major shift in warfighting as we know it
- Technologies making Moon and some planets habitable and easily reachable, thus creating new territorial ambitions, and generating demand for Internet style communication between planets
- Self-repairing and self-reproducing robots using naturally available material and scalable 3D printing

- Complete cyber speed brain-brain communication using brain waves, including transmission and recreation of deep thoughts. This could have a major impact on the language as a mode of communication in personal and professional lives. It could fundamentally change business discussions and C2 in any warfare.
- Superhuman entities that are qualitatively superior to Homo Sapiens. This could happen along one of several paths:
    - Tightly coupled brain-computer hybrid
        - Instant knowledge, rapid computation, and deep thoughts
    - Machine intelligence by itself surpassing human intelligence (ASI)
    - Computer stimulated rapid biological (r)evolution
- Medical advances to make humans essentially immortal
    - Medicines
    - Synthetic organs providing easy replacements of failing/failed human organs
    - In-situ cloning

Some of these changes are clearly monumental and could dramatically alter the society and military conflicts. They could determine a new world order depending on who gets there first. In any case, these and similar potential Black Swans need to be watched for research breakthroughs that suggest that the future is within the next 10 to 15 years.

6 Summary

Section 1 listed a number of important technology trends with potential to have significant impact on the cyber battleground. Section 3 provided more detail on the technology trends and their likely impact on cyber defense and offense. For each trend, this discussion also provided motivation for several S&T goals. As mentioned in Section 1.1, the report is focused on defensive cyber although S&T for offensive counterpart is as important.

6.1 Trends of Special Interest

The trends and influences discussed in this report are all important to be addressed via S&T. Some of the trends and the strength of their impacts seem easy to anticipate using the extrapolations of the histories of relevant technologies, even if the some of the details will unfold over time. Some other trends as well as the required S&T were not quite as easy to anticipate, and they need special attention. Among broad trends, increasing automation, complexity, programmability, virtualization, and opacity of sourcing is one set of such trends. They influence almost all cyberspace technologies and applications, supply chains, and required reaction time. The second set arises from the increasing tighter relationships between various cyberspace technologies (e.g., cyber and ML) and between cyberspace and application domains (e.g., cyber and physical). These relationships requite interdisciplinary S&T focused on the challenges and opportunities at their intersections. Among technology specific trends, microelectronics, IoT, (semi)-autonomous platforms, digital persona, DDC, and ML are likely to create important new challenges and opportunities. On the applications side, the confluence of IoT sensors using low SWaP-C devices, increasing networking speed, and advancement in computing will accelerate the use of data driven control in all critical infrastructures, mobile platforms, weapons systems, healthcare, and robotics. This increasing pace of transformation of physical systems to smart CPS will lead to improved performance and automation, while adding a new set of vulnerabilities. Integration of inorganic (cyber and physical) with organic (bio and neuro) will lead to a fundamental shift in the human-machine teaming techniques and in the cyber battleground.

Some aspects of Quantum technologies and cyber-physical-bio-neuro integration could have monumental impacts on the cyber battleground. However, there is a very large degree of uncertainty in if and when. Futuristic projections discussed in Section 5 have even more uncertainty. All of these should be watched for sudden and unexpected acceleration to avoid major surprises.

7 Observations and Insights That May Need Separate Studies

During this study, the team encountered sentiments that, while not within the scope of this study, are important enough to be highlighted here. These may need separate studies.

COTS vs GOTS vs Custom DoD technologies: The team noticed a strong sentiment from many experts that the DoD has become too dependent on COTS cyberspace technologies and has little in the way of customization for the DoD needs and differentiators from what COTS technologies provide everyone else. There was a feeling that this move is introducing serious security risks given that the business models of commercial industry may not always value cybersecurity as much as what the DoD needs. Overall, there is a sentiment that the DoD should lead more and have more customization in specific areas, cyber being one.

Loss of Leadership in Critical Technologies:

Another major concern was the loss of leadership in critical areas like microelectronics manufacturing, 5G, ML, ML hardware, and quantum. One result is an unreliable and untrustworthy supply chain for almost all critical hardware. The other result is the possibility of losing intellectual property leadership and important battles before they begin. There was a sentiment that the situation is bad and will become worse in absence of significant increases in S&T investments in these areas. The new investments should drive towards regaining and maintaining leadership, bringing back critical design and manufacturing capabilities, and becoming self-sufficient.

> *In the future, when weapon systems need leading-edge IC to stay competitive against adversaries, DoD will likely need to rely on an unsecure supply chain in another country to meet those needs.-IDA report on 'Supply Chain Risks in Integrated Circuits'*
>
> *China, in particular, is pouring enormous resources into ML and has a long history of using cyberattacks for political and economic aims. Unless the US makes an unprecedented and urgent investment in ML for cyber defense and attack, we will lose the race before it has hardly begun – Dr. H.Kautz, NSF*

8 Study Team

Appendix 1: Core Study Team

The following core team members contributed to the study.

Name	Affiliation
Ryan Craven, CoI WG Lead	Navy/ONR
Bharat Doshi, Study Lead and Lead Author	Navy/ONR
Joseph Mathews	Navy/NRL
Alexander Kott	Army/ARL
Robert Kimball	Army/C5ISR
Paul Robb	Army/C5ISR
Adam Cardinal-Stakenas	NSA
Daniel Clouse	NSA
Marc Lovend	NSA
Emmanuel Bello-Ogunu	MITRE
Joshua Jenks	MITRE

Ms. Alexandra Landsberg (Navy/ONR), as the Cyber CoI Steering Group Lead, provided guidance throughout this study. Mr. Giorgio Bertoli (Army/C5ISR) championed this study when he was the SG Lead.
Mr. Chad Heitzenrater from AFRL provided extensive and valuable feedback on a prior draft of this report.

The core team members reached out to many members in their native organizations when desired.

9 External Experts Who Provided Inputs via Interviews and/or Responses to Questionnaires

The following individual experts and organizations provided inputs via interviews and responses to survey questionnaires. They are listed with functions or the areas of expertise. In addition to the list of sources below, the team also used information collected by the External Influences Subcommittee of the Cyber Roadmap Working Group (CRWG). In particular, the report refers to statements by Battelle and Raytheon-CODEX in response to an RFI, and by Peter Singer and Paul Saffo during interviews. It should be noted that the views expressed in this report are distilled by the team members based on the inputs from all the sources discussed in Section 2, including the expertise within the team. There is no attempt to reflect all viewpoints on any particular topic.

	Name and Method for Obtaining Information	Affiliation	Function/Expertise
Industry	Response to survey questionnaire	Advanced Systems Development, Inc. (ASD)	ML, Cognitive Detection
	Response to survey questionnaire	Assured Information Security, Inc. (AIS)	Secure access to classified data/information over untrusted network
	Response to survey questionnaire	Black Horse	Quantum Resistant Cryptographic migration
	Response to survey questionnaire	Black Sands, Inc.	Secure Connections as a Service (SCaaS)
	Response to survey questionnaire	Grimmer Technology and Operations, Inc. (GROi)	Transport Access control
	Response to survey questionnaire	InfoFusion Corporation	Information fusion for Cyber Situation Awareness (Cyber SA). ML
	Response to survey questionnaire	Modus Operandi, Inc.	Anomaly detection in IoT, Deep Learning
	Response to survey questionnaire	OST	ML for Detection and Response
	Response to survey questionnaire	Parson	Enterprise Network Visualization, 5G
	Response to survey questionnaire	ESRI ArcGIS	Creation, management, and dissemination of maps and spatial information
	Response to survey questionnaire	Sealing Tech	Lightweight Containerized open-source cyber defense service
	Response to survey questionnaire	Soar Technology, Inc.	AI, Cyber Cognitive
	Dileep Bhandarkar, Interview	Retired. QUALCOMM, Microsoft, DEC	Microelectronics and computing Architecture
	Anton Chuvakin, Interview	Google/Gartner	Cyber Physical Systems, Cyber SA, Cyber C2, ML
	Myron Cramer, Response to survey questionnaire	BCT-LLC	CTO, Multiple Technologies
	Response to survey questionnaire	C5 Capital	VC, cyber focus
	Aravind Dasu, Interview	Intel	Microelectronics
	Eric Dull, Interview	Deloitte	ML enabled cyber defense analytics
	Steve Fabian and Larry Frazer, Interview	Cisco	Directors of Engineering and Architecture, Multiple Technologies
	Steven Graves, Response to survey questionnaire	Cornerstone Integration, Inc.	President, Quantum
	Steve Grubman, Interview	McAfee	CTO, Multiple technologies for Cyber security

	John Kindervag and Bruce Marco, Interview	Palo Alto Networks	Cyber security, Zero Trust Strategy, Threats
	Jason Li, Interview	Siege Technologies	Multiple Technologies
	Dave Mihelcic, Interview	Independent Consultant, Formerly CTO of DISA and Juniper Networks	Cyber
	Adam Meyers, Interview	Crowdstrike	Cyber Threat Intelligence
	Jim Mollenkopf, Interview	Qualcomm	VP, Strategy Development
	Vern Solberg, Response to survey questionnaire	Solberg Technical Consulting	Microelectronics packaging
	Brad Spengler, Interview	Open Source Security Inc.	Automatic exploit generation, side channels
	Christopher Valentino, Survey Response	Northrup Grumman	VP of IW & Cyber Survivability, multiple technologies
Academia	Professor Ehab Al-Shaer, Interview	Carnegie Mellon University	Cyberspace technologies
	Professor Chase Cotton, response to survey questionnaire	University of Delaware	Cyber defense
	Professor Sushil Jajodia, Interview	George Mason University	Cyber defense
	Professor Patrick McDaniel, Interview	Pennsylvania State University	Cyber defense, networking
	Professor Alina Oprea, response to survey questionnaire	Northeastern University	Cyber defense
	Professor Robert Simon, , response to survey questionnaire	George Mason University	Secure computing and protocols
	Professor Lauren Zabierek, Interview	Harvard's Belfer Center	Cyber defense and data policies
	Professor Dongyan Xu, Interview	Purdue University	CPS, Formal Methods, cyber resilience
	Professor Zhiyun Qian, , response to survey questionnaire	University of California, Riverside	Computer and network Security
US Government	Frank Acker, Interview	NSA	SDN, IoT, 5G
	Dr. Jeff Alstott, Interview	IARPA	ML/DL
	Giorgio Bertoli, response to survey questionnaire	Army	Cyber defense and offense
	DR. Jill Crisman, Interview	USD (R&E)	AI and ML
	Jeff Kleck, Kate Pfeiffer, Johnson Wu, Interview and , response to survey questionnaire	DIU	Multiple
	Peter Gadford	Army	Microelectronics
	Dr. Simson Garfinkel	Census Bureau	Computer security, privacy
	Dr. Kamal Jabbour, Interview	Air Force	Cyber
	DR. Henry Kautz, Survey Response	NSF	Division Director, IIS, ML
	Dr. Mark Linderman, Interview	Air Force	Cyber, C4I
	Dr. Paul Lopata, Interview	USD (R&E)	Quantum, cyber
	Dr. Ray Richards, Interview	DARPA	Formal Methods and assured software, embedded systems
	Dr. Ananthram Swami, Interview	Army	Networks, Cyber
	Cara Steib and Olga Ratsimor, Interview	NSA	Networks, 5G
	Dr. Cliff Wang, Interview	Army	Cyber
	Dr. Neal Ziring, Interview	NSA	Cyber
FFRDC/UARC	Dr. Doug Ghormley, Interview	Sandia	Software security, autonomy
	Mark Gouker, Response to survey questionnaire	MIT-LL	Microelectronics

	Dr. Wen Masters, Response to survey questionnaire	GTRI	Multiple
	Matt Mickelson Interview	MITRE	Multiple
	Bryan Miller, Interview	Penn State ARL	Cyber-Physical Systems, Cyber-EW
	Dr. George Roelke, Interview	MITRE	Multiple
	Dr. James Schatz, Interview	JHU/APL	Multiple
	Ray Yuan and Team, Interview	JHU/APL	Cyber
	Dr. Matt Gaston, Interview	SEI	Multiple
	Response to survey questionnaire	MITRE	Multiple

10 Abbreviations

Abbreviation	Term
5G	5th Generation of Cellular Wireless Networks
6G	6th Generation of Cellular Wireless Networks
AGI	Artificial General Intelligence
AI	Artificial Intelligence
ANI	Artificial Narrow Intelligence
ASI	Artificial Super Intelligence
ASIC	Application-Specific Integrated Circuit
BDA	Battle Damage Assessment
C2	Command and Control
C4ISR	C4 Intelligence Surveillance and Reconnaissance
CBN	Content Based Networking
CoI	Community of Interest
CONOPs	CONcept of OPerations
COTS	Commercial-Off-The-Shelf
CPS	Cyber-Physical Systems
CSP	cloud service provider
CRWG	Cyber Roadmap Working Group
DARPA	Defense Advanced Research Projects Agency
DCO	Defensive Cyberspace Operations
DDC	Deceptive Digital Content
DDoS	Distributed Denial-of-Service
DEPSECDEF	Deputy Secretary of Defense
DIB	Defense Industrial Base
DIU	Defense Innovation Unit
DL	Deep Learning
DNN	Deep Neural Networks
DoD	Department of Defense
DRL	Deep Reinforcement Learning
FE	Functional Encryption
FHE	Full Homomorphic Encryption
FFRDC	Federally Funded Research & Development Center
FNC3	Fully-Networked Command, Control, and Communications
FPGA	Field-programmable gate array
FV	Formal Verification
FW	Firmware
GAN	Generative Adversarial Networks

Abbreviation	Term
GML	Generative Machine Learning
HE	Homomorphic Encryption
HIL	Human-In-the-loop
HMT	Human-ML Teaming
HW	Hardware
HOL	Human On the Loop
IO	Information Operations
IoT	Internet of Things
IP	Internet Protocol
IPB	Intellectual Property Block
ISA	Instruction Set Architecture
ISP	Internet Service Provider
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
IW	Information Warfare
LEO	Low Earth Orbit (Satellite)
M&S	Modeling and Simulation
ME	Microelectronics
ML	Machine learning
MLaaS	Machine Learning as a Service
MTD	Moving Target Defense
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NSA	National Security Agency
OCO	Offensive Cyber Operations
OODA	Observe–Orient–Decide–Act (as in OODA loop)
OT	Operational Technology
OUSD(R&E)	Office of the Undersecretary of Defense for Research and Engineering
PD	Principal Director
PNT	Position, Navigation & Timing
PPS	Privacy Preserving Search
QC	Quantum Computing
QRE	Quantum Resistant Encryption
R&D	Research and Development
RFI	Request for Information
RL	Reinforcement Learning
RoT	Root of Trust
S&T	Science and Technology
SA	Situational Awareness
SCADA	Supervisory Control And Data Acquisition
SDD	Spatial Diversity Defense
SDN	Software Defined Networks
SDR	Software Defined Radio
SDx	Software-Defined Everything
SMPC	Secure Multi-Party Computation
SoC	System on a Chip

Abbreviation	Term
SW	Software
SWaP	Space, Weight and Power
SWaP-C	Space, Weight and Power –Cost
TCP/IP	Transmission Control Protocol/Internet Protocol
TPU	Tensor Processing Unit
UARC	University Affiliated Research Center
USCYBERCOM	United States Cyber Command
USD(R&E)	Undersecretary of Defense for Research and Engineering
USG	United States Government
VEO	Violent Extremist Organization
VE	Virtual Entity
VM	Virtual Machine
VR	Virtual Reality
XaaS	Everything/Anything as a Service
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZTS	Zero Trust Strategy

11. References

11.1. Microelectronics and Hardware

1. AI in the data center: Harnessing the power of FPGAs – AI Business eBook Series (in collaboration with Xilinx), 2020
2. Gwennap, Linley. (2020) Forbes October 12, 2020. Apples 5 Nanometer Chip Is Another Signpost That Moore's Law Is Running Out. https://www.forbes.com/sites/linleygwennap/2020/10/12/apple-moores-law-is-running-out/
3. Boutros, A. You Cannot Improve What You Do not Measure: FPGA vs. ASIC Efficiency Gaps for Convolutional Neural Network Inference – FPGA vs ASIC
4. Cloud computing FPGA applications - Intel® FPGA. (n.d.). Retrieved April 13, 2021, from https://www.intel.com/content/www/us/en/products/docs/storage/programmable/applications/cloud.html
5. Several DARPA and IARPA programs:
    a. TIC (IARPA) – Disaggregate ASICs into non-functional parts
    b. VAPR: Shatter lost, misplaced, or end-of-life ASICs on command
    c. SPADE: Use secure parts to monitor commercial components packaged together into a single ASIC
    d. DAHI: Disaggregate ASICs into functional subcomponents
    e. CHIPS: Establish a library of pre-verified, modular ASIC design IP
    f. CRAFT: Apply modularity to reduce ASIC design effort and allow portability across foundries
    g. eFuses: Obscure ASIC functionality until after manufacture
    h. SHIELD: Authenticate ASICs at any point in the supply chain
    i. IRIS: Derive an ASICs functionality and reliability
    j. TRUST: Reverse engineer ASICs and compare to design
6. Dennard Scaling - https://en.wikipedia.org/wiki/Dennard scaling
7. Flamm, k., Measuring Moore's Law: Evidence from Price, Cost, and Quality Indexes. University of Texas at Austin (2017) File Download (imf.org)
8. Gwennap, L. (2020, October 13). Apple's 5 Nanometer chip is another signpost that Moore's law is running out. Retrieved April 14, 2021, from https://www.forbes.com/sites/linleygwennap/2020/10/12/apple-moores-law-is-running-out/

9. Henessy, J. and Peterson, D. A New Golden Age for Computer Architecture: Domain-Specific Hardware/Software Co-Design, Enhanced Security, Open Instruction Sets, and Agile Chip Development [John Hennessy and David Patterson Turing Lecture (acm.org)]
10. Henessy, J. and Peterson, D. A new golden age for computer architecture. Communications of the ACM, Volume 62, Issue 2, February 2019 pp 48–60 (2019)
11. LAPEDUS, M., & STEFFORA MUTSCHLER, A. (2020, December 14). Regaining the edge In U.S. chip manufacturing. Retrieved April 13, 2021, from https://semiengineering.com/can-the-u-s-regain-its-edge-in-chip-manufacturing/
12. List of semiconductor fabrication plants. (2021, April 13). Retrieved April 13, 2021, from https://en.wikipedia.org/wiki/List_of_semiconductor_fabrication_plants
13. McGrath, D. (2015, December 02). IC merger mania hits fever pitch. https://www.eetimes.com/ic-merger-mania-hits-fever-pitch/
14. Moore's Law - https://en.wikipedia.org/wiki/Moore%27s_law
15. Platt, S. (2018, October 03). Metamorphosis of an industry, part two: Moore's law and Dennard scaling. https://www.micron.com/about/blog/2018/october/metamorphosis-of-an-industry-part-two-moores-law
16. Shilov, A. (2021, February 10). Samsung Foundry: New $17 Billion fab in the USA by late 2023. Retrieved April 13, 2021, from https://www.anandtech.com/show/16483/samsung-in-the-usa-a-17-billion-usd-fab-by-late-2023
17. Solberg, V. Solberg Technical Consulting. "PCB Designers Guide to Flip-Chip, WLP, FOWLP, 2D, 2.5D, and 3D Semiconductor Package Technologies". IPC APEX Expo 2020 Professional Development Course.
18. Woo, J. (n.d.). Three Dimensional Monolithic System-on-a-Chip (3DSoC). https://www.darpa.mil/program/three-dimensional-monolithic-system-on-a-chip
19. Zhang, P. (2021, March 14). How big is the gap between SMIC and TSMC? Retrieved April 13, 2021, from https://cntechpost.com/2020/07/09/how-big-is-the-gap-between-smic-and-tsmc/

11.2. Networking and Communication

1. A. Aijaz, M. Dohler, A. H. Aghvami, V. Friderikos, and M. Frodigh, *Realizing the Tactile Internet: Haptic Communications over Next Generation 5G Cellular Networks*, in IEEE Wireless Communications, vol. 24, no. 2, pp. 82-89, April 2017.
2. T. Andersen, "Past, Present and Future of Containers", First International Workshop on Container Technologies and Container Clouds, March 2015
3. B. Wang. (2020, February 28). Backdoor [Computer software]. https://github.com/bolunwang/backdoor
4. Bloch, K, "Software defined networks (SDN) - Enabling virtualized, programmable infrastructure", IEEE Conference on Local Computer Networks Workshop October 2013.
5. Andrew T. Campbell, Herman G. De Meer, Michael E. Kounavis, Kazuho Miki, John B. Vicente, and Daniel Villela, "A Survey of Programmable Networks", ACM SIGCOMM Computer Communications Review Volume 29 Issue 2, April 1999
6. Cyber Security and Information Assurance Interagency Working Group Subcommittee on Networking & Information Technology Reseach & Development Committee on Science & Technology Enterprise of the National Science & Technology Council. (2019). Federal Cybersecurity Research and Development Strategic Plan.
7. Dogra A., Jha, R.K., and Jain, S. A Survey on beyond 5G network with the advent of 6G: Architecture and Emerging Technologies (2020), DOI 10.1109/ACCESS.2020.3031234. IEEE Access
8. Lav Gupta, "SDN: Development, Adoption, and Research Trends", www.cse.wustl.edu/~jain/cse570-13/ftp/sdn.pdf
9. N Foster, N McKeown, J Rexford, G Parulkar, *Using deep programmability to put network owners in control*, ACM SIGCOMM Computer Communication Review, October 2020.

10. He, Z., Zhang, T., & Lee, R. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 114-120.
11. Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks (pp. 381-401). Springer International Publishing.
12. Mar, S. "BRINGING CYBERSECURITY INTO THE FUTURE: Internal auditors should consider whether CARTA is a smarter approach to addressing information security risks." Internal Auditor 75.1 (2018): 16-18.
13. T. S. Rappaport et al., *Wireless Communications and Applications above 100 GHz: Opportunities and Challenges for 6G and Beyond,* in IEEE Access, vol. 7, pp. 78729-78757, 2019.
14. Special Issue: Software-Defined Networks, IEEE The Institute, December 2014
15. Srndic N., Laskov, P. "Practical Evasion of a Learning-Based Classifier: A Case Study," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 197-211, doi: 10.1109/SP.2014.20.
16. Staff, N. (2020, December 09). NSA cybersecurity perspectives on quantum key distribution and quantum cryptography. https://www.quantum.gov/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptography/
17. Vamosi, R. (2013). NSA Experimenting with BYOD. Retrieved April 14, 2021, from https://www.mocana.com/blog/2013/02/27/nsa-experimenting-with-byod
18. Vermeer, M. "Securing Communications in the Quantum Computing Age." RAND Corporation, 9 Apr. 2020, www.rand.org/pubs/research_reports/RR3102.html

11.3. Core Computing (GPU, TPU, Multi-core, parallel, Custom)

1. Misic, M., Dudevic, D., and Tomasevic, M. *Evolution and trends in GPU Computting.* 2012/DC-VIS
2. Graphics Processing Unit. https://en.wikipedia.org/wiki/Graphics_processing_unit
3. GPU Benchmarks and Hierarchy 2021: Graphics Cards Ranked. https://www.tomshardware.com/reviews/gpu-hierarchy,4388.html
4. Tensor Processing Unit. https://en.wikipedia.org/wiki/Tensor_Processing_Unit
5. Understanding Tensor Processing Unit. https://medium.com/sciforce/understanding-tensor-processing-units-10ff41f50e78
6. Tensor Processing Unit. https://semiengineering.com/knowledge_centers/integrated-circuit/ic-types/processors/tensor-processing-unit-tpu/
7. Cloud TPU. https://cloud.google.com/tpu
8. Parallel Processing. https://searchdatacenter.techtarget.com/definition/parallel-processing
9. Custom Processors. https://cccp.eecs.umich.edu/research/past_proc.php
10. Mac Transition to Apple silicon. https://en.wikipedia.org/wiki/Mac_transition_to_Apple_silicon
11. ARM Microarchitecture. https://en.wikipedia.org/wiki/List_of_ARM_microarchitectures

11.4. Cloud Computing

1. Boneh, D., Sahai, A., & Waters, B. (2011). Functional Encryption: Definitions and Challenges. IACR Cryptol. ePrint Arch., 2010, 543.
2. Campbell, M. "Beyond Zero Trust: Trust Is a Vulnerability." Computer 53.10 (2020): 110-113.
3. Cloud computing FPGA applications - Intel® FPGA. (n.d.). https://www.intel.com/content/www/us/en/products/docs/storage/programmable/applications/cloud.html
4. Hassan, W., Chou, T., Omar, T., and Pickard, J., *Cloud Computing Survey On Services, Enhancements And Challenges In The Era Of Machine Learning And Data Science.* International Journal of Latest Trends in Engineering and Technology, Vol.(15), Issue(4), 2020: http://dx.doi.org/10.21172/1.1
5. Shiralkar, T., *Build Resilient, Secure Microservices with Microsegmentation.* The NEWSTACK, 2021, Build Resilient, Secure Microservices with Microsegmentation - The New Stack %

6. Walker, K. "Cloud security alliance announces software defined perimeter (SDP) initiative." Online https://cloudsecurityalliance.org/media/news/csa-announcessoftware-defined-perimeter-sdp-initiative/ (accessed October 2014) (2013).

11.5. Edge Computing

1. Abdelzaher, T., Ayanian, N., Başar, T., Diggavi, S., Diesner, J., Ganesan, D., Govindan, R., Jha, S., Lepoint, T., Marlin, B.M., Nahrstedt, K., Nicol, D., Rajkumar, R., Russell, S., Seshia, S., Sha, F., Shenoy, P., Srivastava, M., Sukhatme, G., Swami, A., Tabuada, P., Towsley, D., Vaidya, N., & Veeravalli, V. (2018). Toward an Internet of Battlefield Things: A Resilience Perspective. Computer, 51, 24-36.
2. Anderson, S. NSA Mobile Devices Security Best Practices NSA Mobile Device Security Best Practices (steveanderson.com)
3. Carr, D., *Edge computing vs. cloud computing: What's the difference?* 2020, The Enterprisers Project.
4. Psaras, I., *Decentralized Edge-Computing and IoT through Distributed Trust.* MobiSys '18: Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services, June 2018, Pages 505–507. https://doi.org/10.1145/3210240.3226062
5. Vamosi, R. (2013). NSA Experimenting with BYOD. https://www.mocana.com/blog/2013/02/27/nsa-experimenting-with-byod
6. Walker, K. "Cloud security alliance announces software defined perimeter (SDP) initiative." online] https://cloudsecurityalliance.org/media/news/csa-announcessoftware-defined-perimeter-sdp-initiative/ (accessed October 2014) (2013).
7. Whitney, L. (2020, September 25). How to TRAIN Amazon's Alexa to recognize your voice. Retrieved April 14, 2021, from https://www.pcmag.com/how-to/how-to-train-amazons-alexa-to-recognize-your-voice
8. Zhang, Q., Jia, S., Chang, B., &amp; Chen, B. (2018, June 05). Ensuring data confidentiality via plausibly deniable encryption and secure deletion – a survey. Retrieved April 14, 2021, from https://cybersecurity.springeropen.com/articles/10.1186/s42400-018-0005-8

11.6. Quantum

1. "A Preview of Bristlecone, Google’s New Quantum Processor." Google AI Blog, 5 Mar. 2018, ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
2. "*ADVANCING QUANTUM INFORMATION SCIENCE: NATIONAL CHALLENGES AND OPPORTUNITIES*." National Archives, A JOINT REPORT OF THE Committee on Science and Committee on Homeland and National Security OF THE NATIONAL SCIENCE AND TECHNOLOGY COUNCIL obamawhitehouse.archives.gov/sites/default/files/quantum_info_sci_report_2016_07_22_final.pdf
3. "Developing a Topological Qubit." Microsoft Quantum, cloudblogs.microsoft.com/quantum/2018/09/06/developing-a-topological-qubit. Accessed 9 Mar. 2021.
4. "DWave: The Quantum Computing Company." DWave Systems, www.dwavesys.com/quantum-computing . Accessed 10 Mar. 2021.
5. Lloyd S., and Englund, D., *Future Directions of Quantum Information Processing.* A Workshop on the Emerging Science and Technology of Quantum Computation, Communication, and Measurement Future Directions Quantum.pdf (defense.gov)
6. "Future Directions of Quantum Information Processing." Office of the Under-Secretary of Defense for Research & Engineering, basicresearch.defense.gov/Portals/61/Documents/future directions/Future_Directions_Quantum.pdf?ver=2017-09-20-003031-450
7. L. Gyongyosi, S. Imre, and H. V. Nguyen, A survey on quantum channel capacities, IEEE Communication Surveys, vol. 20, no. 2, pp. 1149-1205, 2nd Quart., 2018.

8. "IBM Achieves Highest Quantum Volume to Date, Establishes Roadmap for Reaching Quantum Advantage." IBM News Room, newsroom.ibm.com/2019-03-04-IBM-Achieves-Highest-Quantum-Volume-to-Date-Establishes-Roadmap-for-Reaching-Quantum-Advantage.
9. "IBM: Quantum Computing." IBM Quantum, 2 Apr. 2009, www.ibm.com/quantum-computing/
10. "IonQ | Trapped Ion Quantum Computing." IonQ, ionq.com. Accessed 10 Mar. 2021.
11. Staff, N. (2020, December 09). "NSA Cybersecurity Perspectives on Quantum Key Distribution and Quantum Cryptography – National Quantum Initiative." www.quantum.gov/nsa-cybersecurity-perspectives-on-quantum-key-distribution-and-quantum-cryptography .
12. "Post-Quantum Cryptography | CSRC." National Institute of Standards & Technology, csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline.
13. "Quantum Computing." Intel, www.intel.com/content/www/us/en/research/quantum-computing.html . Accessed 10 Mar. 2021.
14. "Rigetti Computing." Rigetti Computing, www.rigetti.com . Accessed 10 Mar. 2021.
15. Arute, F., et al. "Quantum supremacy using a programmable superconducting processor." Nature 574.7779 (2019): 505-510.
16. Aumasson, J. P. (2017). The impact of quantum computing on cryptography. Computer Fraud & Security, 2017(6), 8-11.
17. Create a quantum random number generator - azure quantum. (2021). Retrieved April 14, 2021, from https://docs.microsoft.com/en-us/quantum/tutorials/quantum-random-number-generator?tabs=tabid-qsharp
18. Create a Quantum Random Number Generator - Azure Quantum. Microsoft Docs, docs.microsoft.com/en-us/azure/quantum/tutorial-qdk-quantum-random-number-generator?tabs=tabid-qsharp. Accessed 9 Mar. 2021.
19. Cross, A. W., et al. "Validating quantum computers using randomized model circuits." Physical Review A 100.3 (2019): 032328.
20. Giles, M. (2020, April 02). Explainer: What is a quantum computer? Retrieved April 14, 2021, from https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/
21. Goled, S. "Chinese Researchers Demonstrate World's Largest Stable Quantum Communication Network." Analytics India Magazine, 13 Jan. 2021, analyticsindiamag.com/chinese-researchers-demonstrate-worlds-largest-stable-quantum-communication-network.
22. Gyongyosi, L., Sandor I., and Nguyen, H.V. "A survey on quantum channel capacities." IEEE Communications Surveys & Tutorials 20.2 (2018): 1149-1205.
23. Hartnett, K. "Does Neven's Law Describe Quantum Computing's Rise? | Quanta." Quanta Magazine, 18 June 2019, www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618 .
24. Moll, N., et al. "Quantum optimization using variational algorithms on near-term quantum devices." Quantum Science and Technology 3.3 (2018): 030503.
25. Moskvitch, K. "Gil Kalai's Argument against Quantum Computers." Quanta Magazine, 7 Feb. 2018, www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207 .
26. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). (n.d.). https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/
27. Scarani, V., and Kurtsiefer, C. "The black paper of quantum cryptography: real implementation problems." Theoretical Computer Science 560 (2014): 27-32.
28. Vermeer, M. "Securing Communications in the Quantum Computing Age." RAND Corporation, 9 Apr. 2020, www.rand.org/pubs/research_reports/RR3102.html
29. Wallden, P., and Kashefi, E. "Cyber security in the quantum era." Communications of the ACM 62.4 (2019): 120-120.

11.7. Cyber Physical Systems, including cyberspace technologies in infrastructure, mobile platforms, weapons systems, etc.

1. Y Chen, B Xuan, CM Poskitt, J Sun (2020) Active fuzzing for testing and securing cyber-physical systems- Proceedings of the 29th …, 2020 - dl.acm.org
2. Fabio Cremona, Marten Lohstroh, David Broman, Edward A. Lee, Michael Masin, and Stavros Tripakis, Hybrid Co-simulation: It's About Time, International Journal on Software and Systems Modeling (SoSym), pp 1-25. EECS Tech Report.
3. P Dash, M Karimibiuki, K Pattabiraman (2019)   Out of control: stealthy attacks against robotic vehicles protected by control-based techniques- Proceedings of the 35th Annual …, 2019 - dl.acm.org
4. P Dash, M Karimibiuki, K Pattabiraman (2021) Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques - Digital Threats: Research and …, 2021 - dl.acm.org
5. Patricia Derler, Edward A Lee, Martin Torngren, Stavros Tripakis. "Cyber-Physical System Design Contracts," ACM/IEEE 4th International Conference on Cyber-Physical Systems (ICCPS), Philadelphia, Pennsylvania, April 8 - 11, 2013.
6. Patricia Derler, Edward A. Lee, Alberto Sangiovanni-Vincentelli. "Modeling Cyber-Physical Systems," Proceedings of the IEEE (special issue on CPS), 100(1):13-28, January 2012”.
7. Y Ding, X Zhang, G Wang, F Xu (2016). Joint fingerprinting and encryption in the dwt domain for secure m2m communication. Journal of Security …, 2016 pdfs.semanticscholar.org
8. [IEEE CNS (CPS-Sec)‘20] On the Feasibility of Exploiting Traffic Collision Avoidance System Vulnerabilities (Press: The Register Article)
9. Shamina Hossain-McKenzie, Kaushik Raghunath, Kate Davis, Sriharsha Etigowni, Saman Zonouz, A Strategy for Distributed Controller Defense: Leveraging Controller Roles and Control Support Groups to Maintain or Regain Control in Cyber-Adversarial Power Systems', IET Cyber-Physical Systems: Theory & Applications, 2021
10. Ilge Akkaya, Data-Driven Cyber-Physical Systems via Real-Time Stream Analytics and Machine Learning, PhD Thesis, EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2016-159, October 25, 2016.
11. Jeff C. Jensen, Danica H. Chang, and Edward A. Lee, " A Model-Based Design Methodology for Cyber-Physical Systems," Proceedings of the First IEEE Workshop on Design, Modeling, and Evaluation of Cyber-Physical Systems (CyPhy), Istanbul, Turkey, July 6-7, 2011.
12. Z. Jakovljevic, V. Lesi, S. Mitrovic, and M. Pajic, "Distributing Sequential Control for Manufacturing Automation Systems”, IEEE Transactions on Control Systems Technology, 28(4), 1586-1594, July 2020.
13. I. Jovanov and M. Pajic, "Relaxing Integrity Requirements for Attack-Resilient Cyber-Physical Systems", IEEE Transactions on Automatic Control, 64(12), 4843-4858, December 2019.
14. Kumaraswamy, Y. S. (2014). On autonomic self-healing architecture for resiliency in cyber physical system. International Journal of Multimedia and Ubiquitous Engineering, 9(11), 75-84.
15. Lee, E. Cyber-Physical Systems: A Fundamental Intellectual Challenge, Guest Lecture College de France, Paris, France, Dec. 11, 2013v
16. Edward A. Lee and Sanjit A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach, Second Edition, MIT Press, ISBN 978-0-262-53381-2, 2017.
17. Edward A. Lee, Jan Reineke, and Michael Zimmer, "Abstract PRET Machines," Invited TCRTS award paper. IEEE Real-Time Systems Symposium (RTSS 17), December 5, 2017.
18. E. A. Lee, "CPS Foundations," in Proc. Design Automation Conference (DAC), ACM, 2010.
19. Edward A. Lee, Slobodan Matic, Sanjit A. Seshia, Jia Zou. "The Case for Timing-Centric Distributed Software," IEEE International Conference on Distributed Computing Systems Workshops: Workshop on Cyber-Physical Systems, IEEE, pp. 57-64, June, 2009.

20. Edward A. Lee, "Cyber Physical Systems: Design Challenges," International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), May, 2008; Invited Paper.
21. Edward A. Lee, Fundamental Limits of Cyber-Physical Systems Modeling, ACM Transactions on Cyber-Physical Systems, vol. 1, no. 1, Article 3, November, 2016.
22. Edward A. Lee, Mehrdad Niknami, Thierry Nouidui, Michael Wetter "Modeling and Simulating Cyber-Physical Systems using CyPhySim," in Proceedings of the International Conference on Embedded Software (EMSOFT), Amsterdam, The Netherlands, October 4-9, 2015.
23. Edward A. Lee, "The Past, Present, and Future of Cyber-Physical Systems: A Focus on Models," Sensors, 15(3), pp. 4837-4869, doi:10.3390/s150304837, February, 2015.
24. Edward A. Lee. "Constructive Models of Discrete and Continuous Physical Phenomena," IEEE Access, Vol.2, pp. 797-821, August 7, 2014.
25. Sriharsha Etigowni, Sizhuang Liang, Saman Zonouz, Raheem Beyah, Physics-Aware Security Monitoring against Structural Integrity Attacks in 3D Printers, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2021.
26. V. Lesi, Z. Jakovljevic, and M. Pajic, “Synchronization of Distributed Controllers in Cyber-Physical Systems”, 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019.
27. V. Lesi, Z. Jakovljevic, and M. Pajic, "Towards Resilient and Reliable Distributed Automation for Smart Manufacturing Systems", Workshop on Smart Manufacturing Modeling and Analysis (SM^{2}N), CPS-IoT Week, 2019.
28. V. Lesi, I. Jovanov, and M. Pajic, "Security-Aware Scheduling of Embedded Control Tasks", ACM Transactions on Embedded Computing Systems, part of the ESWEEK-TECS special issue, the 17th ACM SIGBED International Conference on Embedded Software (EMSOFT), 16(5s), 188:1-188:21, October 2017. (Best Paper Award)
29. Xiaojun Liu, Jie Liu, Johan Eker, and Edward A. Lee, "Heterogeneous Modeling and Design of Control Systems," in Software-Enabled Control: Information Technology for Dynamical Systems, T. Samad and G. Balas (eds.), New York City: IEEE Press, 2002.
30. Mertoguno, J. S., Craven, R. M., Mickelson, M. S., & Koller, D. P. (2019, May). A physics-based strategy for cyber resilience of CPS. In Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019 (Vol. 11009, p. 110090E). International Society for Optics and Photonics.
31. R. Mangharam, H. Abbas, M. Behl, K. Jang, M. Pajic, and Z. Jiang, "Three Challenges in Cyber-Physical Systems", 8th International Conference on Communication Systems and Networks (COMSNETS), 2016.
32. Ali Mazloomzadeh, Osama Mohammed, Saman Zonouz, Empirical Development of a Trusted Sensing Base for Power System Infrastructures, IEEE Transactions on Smart Grid, 2015
33. M. Pajic, O. Sokolsky, R. Alur, R. Mangharam, N. Michael, G.J. Pappas, P. Tabuada, S. Weirich, and I. Lee, "Towards synthesis of platform-aware attack-resilient control systems", 2nd ACM International Conference on High Confidence Networked Systems (HiCoNS), Philadelphia, PA, 2013
34. [NDSS’21] PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles
35. [NDSS’21] Evading Voltage-Based Intrusion Detection on Automotive CAN
36. [PETS’21] Real-time Analysis of Privacy-(un)aware IoT Applications
37. J. Park, R. Ivanov, J. Weimer, M. Pajic, I. Lee, and S.H. Son, "Security of Cyber-Physical Systems in the Presence of Transient Sensor Faults", ACM Transactions on Cyber-Physical Systems, 1(3), 15:1-15:23, May 2017.
38. M. Pomerleau, “ONR moves to protect ships’ systems from cyberattacks,” Sep 23, 2015, GCN, https://gcn.com/articles/2015/09/23/navy-rhimes.aspx
39. A Concept Map for CPS. Ptolemy Project, Berkeley. Cyber-Physical Systems - a Concept Map (berkeley.edu)
40. Redwood, W.O. (2015) Cyber physical system vulnerability research. diginole.lib.fsu.edu
41. Abijeet Sahu, Zeyu Maoi, Patrick Wlazo, Hao Huangi, Kate Davis, Ana Goulart, Saman Zonouz, Multi-Source Multi-Domain Data Fusion for Cyberattack Detection in Power Systems, IEEE Access, 2021.
42. [UbiComp’21] S3: Side-channel Attack on Stylus Pencil Through Sensors
43. United States Cyber Command. (2020). Technical Challenge Problem Set.

44. [USENIX Security'21] Exposing New Vulnerabilities of Error Handling Mechanism in CAN
45. [USENIX Security'21] ATLAS: A Sequence-based Learning Approach for Attack Investigation
46. Y. Wang and M. Pajic, "Supervisory Control of Discrete Event Systems in the Presence of Sensor and Actuator Attacks", 58th IEEE Conference on Decision and Control (CDC), 2019.
47. Weinbaum, C., Parachini, J. V., Girven, R. S., Decker, M. H., & Baffa, R. C. (2018). Perspectives and Opportunities in Intelligence for U.S. Leaders. Rand Corporation. G Walkup (2019) Investigating Attacks on Industrial Control Systems Using Deterministic Replay Simulation. hammer.figshare.com

11.8. IoT

1. Abdelzaher, T., Ayanian, N., Başar, T., Diggavi, S., Diesner, J., Ganesan, D., Govindan, R., Jha, S., Lepoint, T., Marlin, B.M., Nahrstedt, K., Nicol, D., Rajkumar, R., Russell, S., Seshia, S., Sha, F., Shenoy, P., Srivastava, M., Sukhatme, G., Swami, A., Tabuada, P., Towsley, D., Vaidya, N., & Veeravalli, V. (2018). Toward an Internet of Battlefield Things: A Resilience Perspective. Computer, 51, 24-36.
2. Al-Shaer, E., Wei, J., Hamlen, K.W. Wang, C. Towards intelligent cyber deception systems. In: Autonomous cyber deception: reasoning, adaptive planning, and evaluation of honeythings. New York (NY): Springer; 2019.
3. Christopher Brooks, Chadlia Jerad, Hokeun Kim, Edward A. Lee, Marten Lohstroh, Victor Nouvellet, Beth Osyk, Matt Weber. A Component Architecture for the Internet of Things, *Proceedings of the IEEE*, 2018.
4. Colbaugh, R., & Glass, K. (2011, July). Proactive defense for evolving cyber threats. In Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics (pp. 125-130). IEEE.
5. Hokeun Kim, Eunsuk Kang, Edward A. Lee, and David Broman "A Toolkit for Construction of Authorization Service Infrastructure for the Internet of Things," *Proceedings of the 2nd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI)*, Pittsburgh, PA, USA, April 18-21, 2017. Winner of **Best Paper Award**, presented during CPS Week, 2017.
6. Hokeun Kim, Eunsuk Kang, David Broman, and Edward A. Lee, "An Architectural Mechanism for Resilient IoT Services," *Proceedings of the 1st ACM Workshop on Internet of Safe Things (SafeThings 2017)*, Delft, The Netherlands, November 5, 2017.
7. Hokeun Kim and Edward A. Lee, "Locally Centralized, Globally Distributed Authentication and Authorization for the Internet of Things," *IEEE IT Professional* Vol: 9 Issue: 5, pp 27-33, October, 2017.
8. [IoTDI'21] Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information
9. [IoTDI'20] IoTRepair: Systematically Addressing Device Faults in Commodity IoT
10. Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. Computer, 49(12), 70-75.

11.9. Bio and Neuro in cyberspace

1. Binnendijk, A., Marler, T., & Bartels, E. M. (2020). Brain-Computer Interfaces: U.S. Military Applications and Implications, an Initial Assessment. Rand Corporation Research Report
2. Bouskill, K. E., & Smith, E. (2019). Global Health and Security: Threats and Opportunities. RAND Corporation.
3. Hannas, W. C., Chang, H.-M., Wang, J., Aiken, C., & Chou, D. (2020). China AI-Brain Research. Center for Security and Emerging Technology.
4. Herr, A., & Cheney-Peters, L. S. (2015). Between Iron Man and Aqua Man: Exosuit Opportunities in Maritime Operations. Center for a New American.
5. Norris, M. (2020, August 27). Brain-Computer Interfaces are Coming. Will We Be Ready? Rand Corporation. https://www.rand.org/blog/articles/2020/08/brain-computer-interfaces-are-coming-will-we-be-ready.html
6. Revilla, E., & Jesus Saenz, M. (2020, March 18). Designing AI systems with human-machine teams. https://sloanreview.mit.edu/article/designing-ai-systems-with-human-machine-teams/
7. Trevino, M., *Cyber Physical Systems: The Coming Singularity,* Prism 8, Number 3, 2-13.

8. Wang, C., and Lu, Z. "Cyber deception: Overview and the road ahead." IEEE Security & Privacy 16.2 (2018): 80-85.

11.10. AI and Machine Learning

1. Al-Dujaili, A. (2018, September 12). Robust detection of evasive malware - part 1. https://medium.com/alfagroup-csail-mit/robust-detection-of-evasive-malware-part-1-312efc1bccc3
2. Alireza Zarreh, Can Saygin, HungDa Wan, Yooneun Lee, Alejandro Bracho, A game theory based cybersecurity assessment model for advanced manufacturing systems, Procedia Manufacturing, Volume 26, 2018, Pages 1255-1264, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2018.07.162
3. Al-Shaer, E., Wei, J., Hamlen, K.W. Wang, C. Towards intelligent cyber deception systems. In: Autonomous cyber deception: reasoning, adaptive planning, and evaluation of honeythings. New York (NY): Springer; 2019.
4. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371-390). IEEE.
5. Artificial intelligence (AI) in life Sciences market - Growth, Trends, COVID-19 impact, and Forecasts (2021 - 2026). (n.d.). https://www.mordorintelligence.com/industry-reports/artificial-intelligence-in-life-sciences-market
6. Biggio, K. Rieck, D. Ariu, C. Wressnegger, I. Corona, G. Giacinto, F. Roli, Poisoning behavioral malware clustering, in: AISec ’14, ACM, 2014, pp. 27–36., https://arxiv.org/abs/1811.09985
7. D. Rouhani, M. Samragh, M. Javaheripi, T. Javidi and F. Koushanfar, "DeepFense: Online Accelerated Defense Against Adversarial Deep Learning," 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Diego, CA, 2018, pp. 1-8, doi: 10.1145/3240765.3240791. https://arxiv.org/abs/1709.02538
8. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122.
9. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition 84, 317-331.
10. Biggio, B., Rieck, K., Ariu, D., Wressnegger, C., Corona, I., Giacinto, G., & Roli, F. (2014). Poisoning behavioral malware clustering. ArXiv, abs/1811.09985.
11. Biswas, D. (2021, April 06). Federated learning - privacy preserving machine learning. Retrieved April 14, 2021, from https://towardsdatascience.com/federated-learning-privacy-preserving-machine-learning-3eea09761e47
12. Bendale and T. Boult, "Towards Open World Recognition," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 1893-1902, doi: 10.1109/CVPR.2015.7298799. https://arxiv.org/abs/1412.5687
13. Calandrino JA, Kilzer A, Narayanan A, Felten EW, Shmatikov V. 2011. ‘You might also like:’ privacy risks of collaborative filtering. In Proc. of the 2011 IEEE Symp. On Security and Privacy (SP), Oakland, CA, 22–25 May 2011, pp. 231–246. New York, NY: IEEE.
14. CBS News. (2016, June 01). Bill Gates Calls artificial INTELLIGENCE "the holy grail". Retrieved April 14, 2021, from https://www.cbsnews.com/video/bill-gates-calls-artificial-intelligence-the-holy-grail/
15. CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security October 2017 Pages 1125–1142 https://doi.org/10.1145/3133956.3134083
16. CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security November 2019 Pages 2023–2040 https://doi.org/10.1145/3319535.3354206
17. Chen, Y., Nadji, Y., Kountouras, A., Monrose, F., Perdisci, R., Antonakakis, M., & Vasiloglou, N. (2017). Practical Attacks Against Graph-based Clustering. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.
18. Chen, Z., & Liu, B. (2016). Lifelong Machine Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning.
19. Chernikova & Oprea. FENCE: Feasible Evasion Attacks on Neural Networks in Constrained Environment, arXiv: 1909.10480, 2020.

20. Colbaugh, R., & Glass, K. (2011, July). Proactive defense for evolving cyber threats. In Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics (pp. 125-130). IEEE.
21. Copeland, B. (2020, August 11). Artificial intelligence. Encyclopedia Britannica. https://www.britannica.com/technology/artificial-intelligence
22. Corona, I., Giacinto, G., & Roli, F. (2013). Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. Inf. Sci., 239, 201-225.
a. L. Marino, C. S. Wickramasinghe and M. Manic, "An Adversarial Approach for Explainable AI in Intrusion Detection Systems," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, 2018, pp. 3237-3243, doi: 10.1109/IECON.2018.8591457. https://arxiv.org/abs/1811.11705
23. N. Dalvi, P. Domingos, Mausam, S. Sanghai, D. Verma, Adversarial classification, in: Int'l Conf. Knowl. Disc. and Data Mining, 2004, pp. 99–108.
24. De Gaspari, F., Jajodia, S., Mancini, L., Panico, A. AHEAD: a new architecture for active defense. In: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig); 2016.
25. Demontis, et al. Why do adversarial attacks transfer? Explaining transferability of evasion and poisoning attacks, USENIX 2019.
26. Dickson, B. (2020, December 16). Machine learning adversarial attacks are a ticking time bomb. https://bdtechtalks.com/2020/12/16/machine-learning-adversarial-attacks-against-machine-learning-time-bomb
27. DoD adopts ethical principles for artificial intelligence. (2020, February 24). https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
28. Dreossi, T., Ghosh, S., Sangiovanni-Vincentelli, A., & Seshia, S. (2019). A Formalization of Robustness for Deep Neural Networks. ArXiv, abs/1903.10033.
29. Egel, D., Robinson, E., Cleveland, C. T., & Oates, C. (2019, October 31). AI and Irregular Warfare: An Evolution, Not a Revolution.
30. Exec. Order No. 13960, 3 C.F.R. 78939 (2020), https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf
31. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.
32. Ateniese, L. V. Mancini, A. Spognardi, A. Villani, D. Vitali, and G. Felici, "Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers," International Journal of Security and Networks, vol. 10, no. 3, pp. 137–150, 2015
33. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J.W., Wallach, H., Daumé, H., & Crawford, K. (2018). Datasheets for Datasets. ArXiv, abs/1803.09010. https://arxiv.org/abs/1803.09010
34. Goldblum, M., Tsipras, D., Xie, C., Chen, X., Schwarzschild, A., Song, D., Madry, A., Li, B., & Goldstein, T. (2020). Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. ArXiv, abs/2012.10544.
35. GPT-3, MIT Technology Review. https://www.technologyreview.com/2021/02/24/1014369/10-breakthrough-technologies-2021/#gpt3
36. Guidotti, D., Leofante, F., Pulina, L., & Tacchella, A. (2020). Verification of Neural Networks: Enhancing Scalability through Pruning. ECAI.
37. Hannas, W. C., Chang, H.-M., Wang, J., Aiken, C., & Chou, D. (2020). China AI-Brain Research. Center for Security and Emerging Technology
38. He, Z., Zhang, T., & Lee, R. (2017). Machine Learning Based DDoS Attack Detection from Source Side in Cloud. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 114-120.
39. Heinl, C.H. "Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications," in 6th International Conference on Cyber Conflict, Brangetto, P., Maybaum, M. and Stinissen, J., Eds., Tallinn, NATO CCD COE Publications, 2014, pp. 53-66.
40. Hosanagar, K. A human's guide to machine intelligence: how algorithms are shaping our lives and how we can stay in control. Penguin Books, 2020.

41. Hsu, T., Liau, C., Wang, D., & Chen, J.K. (2002). Quantifying Privacy Leakage through Answering Database Queries. ISC.
42. https://arxiv.org/abs/1903.10033 - "A Formalization of Robustness for Deep Neural Network
43. https://www.cs.uic.edu/~liub/lifelong-machine-learning.html
44. https://www.darpa.mil/program/explainable-artificial-intelligence
45. Ilahi, I., Usama, M., Qadir, J., Janjua, M.U., Al-Fuqaha, A., Hoang, D.T., & Niyato, D. (2020). Challenges and Countermeasures for Adversarial Attacks on Deep Reinforcement Learning. ArXiv, abs/2001.09684.
46. Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features, SEC'19: Proceedings of the 28th USENIX Conference on Security Symposium, August 2019, pp 285-302, ISBN: 978-1-939133-06-9
47. International Conference on Machine Learning and Applications (ICMLA), pages 1543–1550. IEEE, 2019
48. Joint Artificial Intelligence Center. (n.d.). Retrieved April 14, 2021, from https://dodcio.defense.gov/About-DoD-CIO/Organization/jaic/
49. Katz G., Barrett C., Dill D.L., Julian K., Kochenderfer M.J. (2017) Reluplex: An Efficient SMT Solver for Verifying Deep Neural Networks. In: Majumdar R., Kunčak V. (eds) Computer Aided Verification. CAV 2017. Lecture Notes in Computer Science, vol 10426. Springer, Cham. https://doi.org/10.1007/978-3-319-63387-9_5
50. King, M. (n.d.). Trojans in Artificial Intelligence (TrojAI). Retrieved April 14, 2021, from https://www.iarpa.gov/index.php/research-programs/trojai
51. Kott, A., & Alberts, D. S. (2017). How do you command an army of intelligent things? Computer, 50(12), 96-100.
52. Kott, A., & Stump, E. (2019). Intelligent autonomous things on the battlefield. In Artificial intelligence for the internet of everything (pp. 47-65). Academic Press.
53. Kott, A., & Theron, P. (2020). Doers, not watchers: Intelligent autonomous agents are a path to cyber resilience. IEEE Security & Privacy, 18(3), 62-66.
54. Kott, A., Théron, P., Drašar, M., Dushku, E., LeBlanc, B., Losiewicz, P., Guarino, A., Mancini, L., Panico, A., Pihelgas, M. and Rzadca, K., 2018. Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. arXiv preprint arXiv:1803.10664.
55. Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.
56. Li, S., et al. Stealthy adversarial perturbations against real-time video classification systems, NDSS 2019
57. Lin, Y., Hong, Z., Liao, Y., Shih, M., Liu, M., & Sun, M. (2017). Tactics of Adversarial Attack on Deep Reinforcement Learning Agents. ArXiv, abs/1703.06748.
58. Langewiesche, W. (2019, September 18). What really brought down the Boeing 737 max? Retrieved April 14, 2021, from https://www.nytimes.com/2019/09/18/magazine/boeing-737-max-crashes.html
59. Lin, Z., Shi, Y., & Xue, Z. (2018). IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection. ArXiv, abs/1809.02077.
60. Liuwan Zhu, Rui Ning, CongWang, Chunsheng Xin, and HongyiWu. Gangsweep: Sweep out neural backdoors by GAN. In Proceedings of the 28th ACM International Conference on Multimedia, pages 3173–3181, 2020
61. Madani, P., Vlajic, N. 2018. Robustness of deep autoencoder in intrusion detection under adversarial contamination. In Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HoTSoS '18). Association for Computing Machinery, New York, NY, USA, Article 1, 1–8. DOI: https://doi.org/10.1145/3190619.3190637
62. Mandal, D., Deng, S., Jana, S., Wing, J.M., & Hsu, D.J. (2020). Ensuring Fairness Beyond the Training Data. ArXiv, abs/2007.06029.
63. Margaret Mitchell, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru. 2019. Model Cards for Model Reporting. In Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT* '19). Association for Computing Machinery, New York, NY, USA, 220–229. DOI:https://doi.org/10.1145/3287560.3287596 https://arxiv.org/abs/1810.03993 , https://research.google/pubs/pub48120/
64. McSherry, F. (2016, June 14). Statistical inference considered harmful. Retrieved April 14, 2021, from https://github.com/frankmcsherry/blog/blob/master/posts/2016-06-14.md

65. Microsoft malware classification Challenge (BIG 2015). (2018). Retrieved April 14, 2021, from https://www.kaggle.com/c/malware-classification
66. Miller, et al. Improving Robustness to Attacks Against Vertex Classification, Mining and Learning with Graphs workshop 2019
67. Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., &amp; Grossman, D. (2020, April 28). Military applications of AI raise ethical concerns. Retrieved April 14, 2021, from https://www.rand.org/pubs/research_reports/RR3139-1.html
68. Motzek, A., Möller, R. "Context- and bias-free probabilistic mission," Computers & Security, vol. 65, pp. 166-186, 2017.
69. N. Dalvi, P. Domingos, Mausam, S. Sanghai, D. Verma, Adversarial classification, in: Int'l Conf. Knowl. Disc. and Data Mining, 2004, pp. 99–108.
70. n.d. (2020, August 06). $16.7 billion AI in manufacturing market assessment 2020-2026 - an explosive growth OF 57.2% CAGR is anticipated. https://www.globenewswire.com/news-release/2020/08/06/2074143/0/en/16-7-Billion-AI-in-Manufacturing-Market-Assessment-2020-2026-An-Explosive-Growth-of-57-2-CAGR-is-Anticipated.html
71. Nguyen, T. T., & Reddi, V. J. (2019). Deep reinforcement learning for cyber security. arXiv preprint arXiv:1906.05799.
72. Papernot, et al. Distillation as a defense to adversarial perturbations against deep neural networks, IEEE SSP 2016
73. Papernot, et al. Practical black-box attacks against machine learning, Asia CCS 2017
74. Papernot, et al. The Limitations of Deep Learning in Adversarial Settings, IEEE Euro S&P 2016
75. Papernot, et al. Transferability in machine learning: from phenomena to black-box attacks using adversarial samples, arXiv 1605.07277, 2016
76. Papernot, N., McDaniel, P., & Goodfellow, I. (2016). Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples. ArXiv, abs/1605.07277.
77. Phillips, P., Hahn, A., Fontana, P., Broniatowski, D., &amp; Przybocki, M. (2021, March 01). Four principles of EXPLAINABLE artificial Intelligence (Draft). Retrieved April 14, 2021, from https://www.nist.gov/publications/four-principles-explainable-artificial-intelligence-draft
78. Piekarski, B., Sadler, B., Young, S., Nothwang, W., & Rao, R. (2016). Research and VIsion for Intelligent Systems for 2025 and Beyond. Small Wars Journal.
79. Michael Postol, Candace Diaz, Robert Simon, and Drew Wicke, *Time-series data analysis for classification of noisy and incomplete internet-of-things datasets,* 2019 18th IEEE
80. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 305-316, doi: 10.1109/SP.2010.25. http://www.icir.org/robin/papers/oakland10-ml.pdf
81. Rakhsha, A., Radanovic, G., Devidze, R., Zhu, X., & Singla, A. (2020). Policy Teaching in Reinforcement Learning via Environment Poisoning Attacks. ArXiv, abs/2011.10824.
82. Revathi, S., & Malathi, A. (2013). A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection. International journal of engineering research and technology, 2.
83. Revilla, E., & Jesus Saenz, M. (2020, March 18). Designing AI systems with human-machine teams. Retrieved April 14, 2021, from https://sloanreview.mit.edu/article/designing-ai-systems-with-human-machine-teams/
84. Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. 2017. Membership inference attacks against machine learning models. In Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 3–18.
85. Ridley, A. "Machine learning for Autonomous Cyber Defense," The Next Wave, vol. 22, no. 1, pp. 7-14, 2018.
86. Rubinstein, B.I., Nelson, B., Huang, L., Joseph, A., Lau, S., Rao, S., Taft, N., & Tygar, J. (2009). ANTIDOTE: understanding and defending against poisoning of anomaly detectors. IMC '09.
87. S. Li et al. Connecting the Dots: Defending against Adversarial Examples via Context Learning, ECCV 2020
88. Senator, T. (n.d.). Lifelong Learning Machines (L2M). https://www.darpa.mil/program/science-of-artificial-intelligence-and-learning-for-open-world-novelty
89. Senator, T. (n.d.). Science of Artificial Intelligence and Learning for Open-world Novelty (SAIL-ON). https://www.darpa.mil/program/science-of-artificial-intelligence-and-learning-for-open-world-novelty

90. Severi, et al. Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers. USENIX 2021
91. Shafiq, M., Tabish, S.M., Mirza, F., & Farooq, M. (2009). PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime. RAID.
92. Sheatsley, et al. Adversarial Examples in Constrained Domains, arXiv 2011.01183, 2020
93. Shiva, S., Dasgupta, D., &amp; Wu, Q. (2010, April 20). Game theoretic approaches to protect cyberspace. https://apps.dtic.mil/sti/citations/ADA519126
94. Slam. (2017, June 16). https://www.microsoft.com/en-us/research/project/slam/
95. Smutz, C., & Stavrou, A. (2012). Malicious PDF detection using metadata and structural features. ACSAC '12.
96. Srndic N., Laskov, P. "Practical Evasion of a Learning-Based Classifier: A Case Study," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 197-211, doi: 10.1109/SP.2014.20.
97. Srndic, N. (2014, December 4). MIMICUS [Computer software]. https://github.com/srndic/mimicus
98. Tabassi, E., Burns, K., Hadjimichael, M., Molina-Markham, A., &amp; Sexton, J. (2019, October 30). A taxonomy and terminology of adversarial machine learning. https://csrc.nist.gov/publications/detail/nistir/8269/draft
99. Tang, R., Du, M., Liu, N., Yang, F., &amp; Hu, X. (n.d.). KDD 2020: An embarrassingly simple approach for Trojan attack in deep neural networks. https://www.kdd.org/kdd2020/accepted-papers/view/an-embarrassingly-simple-approach-for-trojan-attack-in-deep-neural-networks
100. Toews, R. (2020, December 22). 10 AI predictions for 2021. https://www.forbes.com/sites/robtoews/2020/12/22/10-ai-predictions-for-2021/
101. Tramer, et al. Ensemble adversarial training: Attacks and defenses, ICLR 2018
102. Trx14. (2020, December 04). TrojanNet [Computer software]. https://github.com/trx14/TrojanNet
103. Turek, M. (n.d.). Explainable Artificial Intelligence (XAI). https://www.darpa.mil/program/explainable-artificial-intelligence
104. Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: model inversion attacks and data protection law. Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 376(2133), 20180083. https://doi.org/10.1098/rsta.2018.0083
105. Villedieu, J. (2017, July 21). Cyber security: How Cisco uses graph analytics to identify threats. Retrieved April 14, 2021, from https://linkurio.us/blog/cyber-security-how-cisco-use-graph-analytics-to-identify-threats/
106. Vought, R. Office of Management and Budget. (2020, November 17). Guidance for Regulation of Artificial Intelligence Applications (M-21-06).
107. Wang R., Zhang G., Liu S., Chen PY., Xiong J., Wang M. (2020) Practical Detection of Trojan Neural Networks: Data-Limited and Data-Free Cases. In: Vedaldi A., Bischof H., Brox T., Frahm JM. (eds) Computer Vision – ECCV 2020. ECCV 2020. Lecture Notes in Computer Science, vol 12368. Springer, Cham. https://doi.org/10.1007/978-3-030-58592-1_14
108. Wang, B., Yao, Y., Shan, S., Li, H., Viswanath, B., Zheng, H., &amp; Zhao, B. Y. (2019). Neural cleanse: Identifying and mitigating backdoor attacks in neural networks. Retrieved April 14, 2021, from https://people.cs.uchicago.edu/~ravenben/publications/abstracts/backdoor-sp19.html
109. B. Wang. (2020, February 28). Backdoor [Computer software]. Retrieved April 14, 2021, from https://github.com/bolunwang/backdoor
110. X. Wang et al, *The security of machine learning in an adversarial setting: A survey,* Journal of Parallel and Distributed Computing, April 2019
111. Wang, Z., et al. SymTCP: Eluding Stateful Deep Packet Inspection with Automated Discrepancy Discovery, NDSS 2020
112. Y. Li. (2021, April 14). Backdoor-learning-resources [Computer software]. https://github.com/THU-YimingLi/backdoor-learning-resources
113. Yang, C., Wu, Q., Li, H.H., & Chen, Y. (2017). Generative Poisoning Attack Method against Neural Networks. ArXiv, abs/1703.01340.
114. Yizhong Ma, Hui Cao and Jun Ma, "The intrusion detection method based on game theory in wireless sensor network," 2008 First IEEE International Conference on Ubi-Media Computing, Lanzhou, China, 2008, pp. 326-331, doi: 10.1109/UMEDIA.2008.4570911.
115. Yuan, X., He, P., Zhu, Q., & Li, X. (2019). Adversarial Examples: Attacks and Defenses for Deep Learning. IEEE Transactions on Neural Networks and Learning Systems, 30, 2805-2824.

116. Zhou, Y., Kantarcioglu, M., & Xi, B. (2019). A survey of game theoretic approach for adversarial machine learning. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9.
117. Liuwan Zhu, Rui Ning, CongWang, Chunsheng Xin, and HongyiWu. Gangsweep: Sweep out neural backdoors by GAN. In Proceedings of the 28th ACM International Conference on Multimedia, pages 3173–3181, 2020
118. Zhang, P. P. K. Chan, B. Biggio, D. S. Yeung and F. Roli, "Adversarial Feature Selection Against Evasion Attacks," in IEEE Transactions on Cybernetics, vol. 46, no. 3, pp. 766-777, March 2016, doi: 10.1109/TCYB.2015.2415032. https://arxiv.org/abs/2005.12154
119. Zhu, S., et al. You Do (Not) Belong Here: Detecting DPI Evasion Attacks with Context Learning, ACM CoNEXT 2020
120. Zugner, D., & Gunnemann, S. (2019). Adversarial Attacks on Graph Neural Networks via Meta Learning.

11.11. Hyper-automation and autonomy in all aspects of cyberspace

1. Alberts, D. S., and Hayes, R.E. Understanding command and control. ASSISTANT SECRETARY OF DEFENSE (C3I/COMMAND CONTROL RESEARCH PROGRAM) WASHINGTON DC, 2006.
2. Basiri, A., Behnam, A., De Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., Rosenthal, C. (2016). Chaos engineering. IEEE Software, 33(3), 35-41.
3. Erdelyi, B., Ahiskali, M., (n.d.). Management and Orchestration of Autonomous Cyber Things. https://apps.dtic.mil/sti/pdfs/AD1106124.pdf
4. Grimaila, M. R., et al. "Mission assurance: issues and challenges." (2010).
5. Guion, J., Reith, M. "Dynamic cyber mission mapping." IIE Annual Conference. Proceedings. Institute of Industrial and Systems Engineers (IISE), 2017.
6. Hoehn, J. R. Joint All Domain Command and Control (JADC2). Congressional Research SVC Washington United States, 2020.
7. Kindervag, J. "Build security into your network's DNA: The zero trust network architecture." Forrester Research Inc (2010): 1-26.
8. Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks (pp. 381-401). Springer International Publishing.
9. Lyle, D. (2014). The rest of the C2 iceberg. AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST.
10. Mavroeidis, V., and Brule, J. "A nonproprietary language for the command and control of cyber defenses–OpenC2." Computers & Security 97 (2020): 101999.
11. Mohammad, S. M., & Lakshmisri, S. (2018). Security automation in Information technology. INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)–Volume, 6.
12. Theron, P., et al. "Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture." 2018 International conference on military communications and information systems (ICMCIS). IEEE, 2018.
13. Wehner, G., Rowell, J., Langley, J., & Mathews, J. Federated Cybersecurity Policy Arbitration.

11.12. Complexity in cyberspace

1. Alibaba Cloud (September 23, 2000). On the Dilemma of Software Complexity. Software Complexity: Definition, Root Causes, and Potential Solutions | Medium
2. Behringer, Michael (1 March 2011). Network Complexity and How to Deal with It. Network Complexity and How to Deal with it | RIPE Labs
3. Cyberspace Solarium Commission Report (11th March 2020). New White Paper, 19th January, 2021.
4. Cyber Security and Information Assurance Interagency Working Group Subcommittee on Networking & Information Technology Reseach & Development Committee on Science & Technology Enterprise of the National Science & Technology Council. (2019). Federal Cybersecurity Research and Development Strategic Plan.
5. Etheredge, Justin (January 29, 2018) Software complexity is killing us. Software Complexity Is Killing Us - Simple Thread

6. Jensen, Benjamin (9 April, 2020). When Systems Fail: What Pandemics and Cyberspace Tell Us About the Future of National Security - War on the Rocks
7. King, Norman (10th September 2017) CyberSecurity — Complexity Risk | Hacker Noon
8. Phister, Paul W. Jr. (2010-2011) Cyberspace: The Ultimate Complex Adaptive System. The International C2 Journal, VOLUME 4, NUMBER 2, 2010–2011
9. SEFFERS,G. *Technology Cost and Complexity Killing U.S. Signal,* July 2014.
10. Wing, Jeannette, M. (March, 2010) Understanding Network Complexity. Second IEEE International Workshop on Network Science for Communications Networks, San Diego, CA, March 19, 2010

11.13. Third party and open source software and hardware in systems

1. Cobb Michael, Open source code reuse: What are the security implications? (techtarget.com)
2. Helpnet Security (2020) Large vendor ecosystems and low visibility increase third-party cyber risk - Help Net Security
3. Keman Huang, Keri Pearlson, and Stuart Madnick (2021), Is Third-Party Software Leaving You Vulnerable to Cyberattacks?   (hbr.org)
4. Kleinman, Leonard (2020). The Rise of Third Party Digital Risk. (forbes.com)
5. Magemeso, Peter, Third Party Software, Institute of Forensic and ICT Security. Third-Party Software - a Security menace | Institute of Forensics and ICT Security (forensicsinstitute.org)
6. Walsh, Karen (2019). Why Worry about Third Party Cyber Risk?   Zeguro Blog
7. Tungaal Abi Tyas (2020) Third Party Risk Management. Upguard. Why is Third-Party Risk Management important in 2021? | UpGuard
8. Zhao, Yuhang, et al. Evaluation indicators for open-source software: a review. Cybersecurity volume 4, Article number: 20 (2021). Springer Open. Evaluation indicators for open-source software: a review | Cybersecurity | Full Text (springeropen.com)
9. How GitHub Secures Open Source Software (2021). White Paper. How GitHub secures open source software | GitHub Resources
10. Sieze the Open Source Opportunity through Comprehensive Optimized Strategies (2021). Forrester Consulting Study: Seizing Open Source Opportunity | OpenLogic by Perforce
11. Cipot, Boris. (2020). The Risks and Potential Impacts Associated with Open Source. - DevOps.com
12. Morgan Jeremy (2019). Reusable Code: The Good, Bad, and Ugly. - DZone Agile
13. Prole, Ken (2018). Code reuse: How to reap the benefits and avoid the dangers | Code Dx
14. Heinamann, Lars (2012). 2012-effective-and-efficient-reuse-with-software-libraries.pdf (cqse.eu)
15. Gkortzis, Antonios et al. (2021). Journal of Systems and Software, Feb 2021. Software reuse cuts both ways: An empirical analysis of its relationship with security vulnerabilities - ScienceDirect
16. Code Reuse a Peril for Secure Software Development | Threatpost
17. Gkortzis, Antonios et al. A double-edged sword? Software reuse and potential security vulnerabilities. GFS_ICSR_19.pdf (antonisgkortzis.github.io)

11.14. Formal Methods

1. *Formal methods*. https://en.wikipedia.org/wiki/Formal_methods
2. Collins, M. (1998). *Formal methods*. https://users.ece.cmu.edu/~koopman/des_s99/formal_methods/
3. Chong, S., Guttman, J., Datta, A., Myers, A., Pierce, B., Schaumont, P., Sherwood, T., & Zeldovich, N. (2016). *Report on the NSF Workshop on Formal Methods for Security*. ArXiv, abs/1608.00678.
4. Dodds, M. *Three ways formal methods can scale for software security. 2021,* (In)secure magazine.
5. Fisher, K., Launchbury, J., and Richard, R. *The HACMS program: using formal methods to eliminate exploitable bugs.* Philosophical Transaction of Royal Society A. https://doi.org/10.1098/rsta.2015.0401

6. Kulik, T., Dongol, B., Larsen, P., Macedo, H.D., Schneider, S., Tran-Jørgensen, P., and Woodcock, J. *A Survey of Practical Formal Methods for Security. Formal Methods.* Under consideration for publication in Formal Aspects of Computing.

11.15. Zero Trust Architecture

1. Boneh, D., Sahai, A., & Waters, B. (2011). *Functional Encryption: Definitions and Challenges*. IACR Cryptol. ePrint Arch., 2010, 543.
2. Campbell, M. *"Beyond Zero Trust: Trust Is a Vulnerability."* Computer 53.10 (2020): 110-113.
3. *Embracing a Zero Trust Security Model.* NSA Cybersecurity Information. CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF (defense.gov)
4. Keyavi data announces public launch of the company and its leadership team. (2020, March 25). https://www.helpnetsecurity.com/2020/03/26/keyavi-data-launch/
5. Kindervag, J. "Build security into your network's DNA: The zero trust network architecture." Forrester Research Inc (2010): 1-26.
6. NSA Issues Guidance on Zero Trust Security Model > National Security Agency Central Security Service > Article View
7. Rose, S., Borchert, O., Mitchell, S., &amp; Connelly, S. (2021, March 23). Zero Trust Architecture. NIST Special Publication 800-207. https://www.nist.gov/publications/zero-trust-architecture

11.16. Preventing compromise from cyber attacks

1. Colbaugh, R., & Glass, K. (2011, July). Proactive defense for evolving cyber threats. In Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics (pp. 125-130). IEEE
2. Y. Li. (2021, April 14). Backdoor-learning-resources [Computer software]. Retrieved April 14, 2021, from https://github.com/THUYimingLi/backdoor-learning-resources

11.17. Autonomic cyber resilience

1. Al-Shaer, E., Wei, J., Hamlen, K.W., Wang, C. Towards intelligent cyber deception systems. In: Autonomous cyber deception: reasoning, adaptive planning, and evaluation of honeythings. New York (NY): Springer; 2019.
2. Basiri, A., Behnam, A., De Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., Rosenthal, C. (2016). Chaos engineering. IEEE Software, 33(3), 35-41
3. Zhao, X., Borders, K., & Prakash, A. (2005). Towards protecting sensitive files in a compromised system. Third IEEE International Security in Storage Workshop (SISW'05), 8 pp.-28.
4. Attivo Networks, https://attivonetworks.com/product/deception-technology/
5. Jajodia, S., Ghosh, A. K., Swarup, V., Wang, C., & Wang, X. S. (Eds.). (2011). Moving target defense: creating asymmetric uncertainty for cyber threats (Vol. 54). Springer Science & Business Media.
6. Dionisio de Niz, "YOLO Transition to Navy Systems ", RHIMES PI Meeting March 12-13, 2019

11.18. Controllability, Predictability, and effectiveness in Offensive Cyber

1. Bertoli, G., & Marvel, L. (2016, January 21). A proposed collateral effect potential metric for computer exploits. Retrieved April 14, 2021, from https://www.slideshare.net/afcea/a-proposed-collateral-effect-potential-metric-for-computer-exploits-technet-augusta-2015
2. Bertoli, G., & Marvel, L. (2018, July 31). Cyberspace Operations Collateral Damage - Reality or Misconception? Retrieved April 14, 2021, from https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Cyberspace%20Operations%20Collateral%20Damage_Bertoli_Marvel.pdf?ver=2018-07-31-093725-187

11.19. Cyber SA and Cyber C2

1. S. Musman, S., Temin, A., Tanner, M., Fox, D., Pridemore, B. "Evaluating the impact of cyber-attacks on missions," in Proceedings of the International Conference on Information Warfare and Security, 2010.
2. Smutz, C., & Stavrou, A. (2012). Malicious PDF detection using metadata and structural features. ACSAC '12.
3. S Zhou, M Möser, Z Yang, B Adida, T Holz. (2020) *An ever-evolving game: Evaluation of real-world attacks and defenses in ethereum ecosystem*- 29th {USENIX} Security ..., - usenix.org
4. Noel, S., L. Jackson, L., Jain, P., Johnson, D., Thomas, R., McFarland, J., King, B., Webster, S., Tello, B. "Analyzing mission impacts of cyber actions (AMICA)." In NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact. 2015.
5. Kott, A., Ludwig, J., & Lange, M. (2017). Assessing mission impact of cyberattacks: toward a model-driven paradigm. IEEE Security & Privacy, 15(5), 65-74.

11.20. Futuristic projections

1. Herr, A. (2015). Will Humans Matter in the Wars of 2030? JFQ 77, 2nd Quarter, 76-83.
2. Herr, A., & Cheney-Peters, L. S. (2015). Between Iron Man and Aqua Man: Exosuit Opportunities in Maritime Operations. Center for a New American.
3. Piekarski, B., Sadler, B., Young, S., Nothwang, W., & Rao, R. (2016). *Research and VIsion for Intelligent Systems for 2025 and Beyond*. Small Wars Journal.
4. Singer, P. W. The Future of War.

11.21. Others

1. Arraj, V. (2010). ITIL®: the basics. Buckinghampshire, UK.
2. Basiri, A., Behnam, A., De Rooij, R., Hochstein, L., Kosewski, L., Reynolds, J., Rosenthal, C. (2016). Chaos engineering. IEEE Software, 33(3), 35-41.
3. Black, J., and Lynch, A. "Cyber Threats to NATO from a Multi-Domain Perspective." Cyber Threats and NATO 2030: Horizon Scanning and Analysis (2020): 126.
4. Bouskill, K. E., & Smith, E. (2019). Global Health and Security: Threats and Opportunities. RAND Corporation.
5. Clarke, R. A., and Knake, R.K. The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats. Penguin Press, 2019.
6. Corporation, I. (2021). Key Terrain Cyber Survey for Industry.
7. Dempsey, K. L., Johnson, L. A., Scholl, M. A., Stine, K. M., Jones, A. C., Orebaugh, A., ... & Johnston, R. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations.
8. Edgar, T. W., & Manz, D. O. (2017). Research methods for cyber security. Syngress.
9. Egel, D., Robinson, E., Cleveland, C. T., & Oates, C. (2019, October 31). AI and Irregular Warfare: An Evolution, Not a Revolution.

10. Gates, B. (2002). Bill Gates: Trustworthy Computing. Retrieved April 14, 2021, from https://www.wired.com/2002/01/bill-gates-trustworthy-computing/
11. Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating Cyberattack in history. Retrieved April 14, 2021, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
12. Hannas, W. C., Chang, H.-M., Wang, J., Aiken, C., & Chou, D. (2020). China AI-Brain Research. Center for Security and Emerging Technology.
13. Hossier, M. (2020). The Joint Officer in the Next War Better Know His Cyber, and Good! Methods to Integrating Cyberspace Operations into Joint Planning. NAVAL WAR COLLEGE NEWPORT RI NEWPORT United States.
14. International Organization for Standardization. ISO/IEC 27000: 2018: Information Technology - Security Techniques - Information Security Management Systems – Overview and Vocabulary. International Organization for Standardization. (2018)
15. Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (as amended through 15 March 2014), 45.
16. Langewiesche, W. (2019, September 18). What really brought down the Boeing 737 max? https://www.nytimes.com/2019/09/18/magazine/boeing-737-max-crashes.html
17. Leonhard, G. (2020, August 10). 2021 will bring the Great American Pivoting: https://www.futuristgerd.com/2020/08/2021-will-bring-the-great-american-pivoting/
18. Meeker, M. "Internet trends report; 2019." (2019).
19. National Science & Technology Council. "2019 Federal Cybersecurity R&D Strategic Plan 2019." The Networking and Information Technology Research and Development (NITRD) Program, NITRD, Dec. 2019, www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf.
20. Osborn, B., et al. "BeyondCorp: Design to deployment at Google." (2016).
21. Paris Call For Trust and Security in Cyberspace (2018)
22. Reveron, D.S. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain", Oxford Press Pg 42 2015.
23. Schneider, Fred B, and U.S. Committee on Information Systems Trustworthiness National Research Council. Trust in Cyberspace. Washington, D.C.: National Academy Press, 1999.
24. Weinbaum, C., Parachini, J. V., Girven, R. S., Decker, M. H., & Baffa, R. C. (2018). Perspectives and Opportunities in Intelligence for U.S. Leaders. Rand Corporation