Science and Technology Law Review

Volume 23 | Number 2 Article 2

2020

Quantum Supremacy, Network Security & the Legal Risk Management Framework: Resiliency for National Security Systems

Salah E. Ali
United States Marine Corps, salahudin.e.ali@gmail.com

Quantum Supremacy, Network Security & the Legal Risk Management Framework: Resiliency for National Security Systems

*Salahudin E. Ali**

> Our Sycamore [sic] processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years.[1]
>
> We want to make our defenses so good, and our architectures so strong, that we do not care whether we are being attacked most of the time because the attacks have no serious effects.[2]

I. INTRODUCTION

In late 2019, Google announced that it had achieved "Quantum Supremacy"[3]—the ability for a quantum computer to solve problems exponentially faster than any existing classical computer.[4] The achievement was accomplished under the backdrop of a heated competition between great powers in a race to achieve this feat.[5] This recent development and break-

---

* Judge Advocate, USMC. LL.M., 2018, The Scalia School of Law at George Mason University; J.D., 2011, Lewis & Clark Law School. The comments in this Article are those of the author and are not associated with the Department of Defense or any other government agency. All errors are his own. All sources used herein for the purposes of this article are unclassified or declassified. The author understands that the existence of classified sources may impact the article's analysis.

1. Frank Arute et al., *Quantum Supremacy Using a Programmable Superconducting Processor*, 574 NATURE 505, 505–11 (2019), https://www.nature.com/articles/s41586-019-1666-5.pdf.
2. RICHARD A. CLARKE & ROBERT K. KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 14 (2019).
3. *Id.*
4. Salahudin Ali, *Coming to a Battlefield Near You: Quantum Computing, Artificial Intelligence, & Machine Learning's Impact of Proportionality*, 18 SANTA CLARA J. INT'L L. 1, 9 (2020) (explaining that quantum computers are those computers that use principles of quantum physics, mechanics, and information science for increased computational power and speed; by contrast, classical computers use individual electronic signals and voltages, via algorithm, in limited binary states).
5. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-656, CONSIDERATIONS FOR MAINTAINING U.S. COMPETITIVENESS IN QUANTUM COMPUTING, SYNTHETIC BIOLOGY, AND OTHER POTENTIALLY TRANSFORMATIONAL RESEARCH AREAS 1 (2018), https://www.gao.gov/assets/700/694748.pdf.

through in quantum computing, although highly criticized,[6] is something to be applauded. For the national security community, however, such applause may be short lived as a reminder of yet another looming cybersecurity threat.[7] Indeed, Quantum Supremacy, with its quantum computing methodology, may pose an existential threat to National Security Systems (NSSs)—information systems that hold and manage national security data—if such systems are ill-prepared to protect such data with what may become outdated security standards.[8]

Current regimes that govern standards and frameworks for protecting national security data may need fresh, new ideas to remain resilient and ensure appropriate decisions can be made that withstand malicious use of new breakthroughs such as quantum supremacy's advanced computing methodology. The current focus remains on technical mitigation of threats encouraged by normative behavior through a risk management framework (RMF).[9] This may not be powerful enough to incentivize behavior which recognizes that new threats are present. A question remains as to what happens after risk has been mitigated but has simultaneously exploited a NSS. New ideas such as providing for decision-making as a legal duty via normative behavior may promote the concept of resiliency, the ability to absorb negative impacts to a NSS while remaining operable, and enables a mindset to "carry-on" when faced with such negative impacts. In other words, there is an expectation of operating in chaos.[10]

The Legal Risk Management Framework (LRMF)—the collection of public laws, statutory, and regulatory requirements mandated or adopted for the protection of information systems by federal agencies—provides an authoritative platform for technical management of risk separate from the RMF.[11] But, as mentioned above, what may be needed is more emphasis on

6. *See, e.g.*, Emily Conover, *Google Officially Lays Claim to Quantum Supremacy*, ScienceNews (Oct. 23, 2019, 4:33 AM), https://www.sciencenews.org/article/google-quantum-computer-supremacy-claim; Kevin Hartnett & Quanta, *Why Two Tech Giants Are Arguing About Quantum Computers*, Atlantic (Oct. 24, 2019), https://www.theatlantic.com/technology/archive/2019/10/why-google-and-ibm-are-arguing-about-quantum-computing/600625/.

7. Scott Buchholz et al., *The Realist's Guide to Quantum Technology and National Security*, Deloitte (Feb. 6, 2020), https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html#.

8. *Id.*

9. *See* Dep't of Def., Instruction No. 8510.01, Risk Management Framework for DoD Information Technology (IT) (2017) [hereinafter Risk Management Framework].

10. Clarke & Knake, *supra* note 2, at 14–15.

11. 44 U.S.C. §§ 3551–3557 (2014); 40 U.S.C. § 11331 (2002); 10 U.S.C. §§ 2223–2224a (2004); Exec. Order No. 12333, 46 Fed. Reg. 59,941 (1981);

legal regimes which focus on and address resiliency when impacted by such risk. This will require a change in thinking about the LRMF as an authoritative legal regime, as compared to a system of normative cybersecurity behaviors found in the RMF, as well as additions to the LRMF and the use of other existing legal regimes to multiply its effectiveness. This proposition promotes contingency plans for information system operability. These new ideas would become part of an authoritative legal regime. If so, solutions may be present to combat emerging threats such as quantum computing (and a variety of other advanced computing threats), thus providing the appropriate level of resiliency for national security systems.

This Article seeks to provide such recommendations by using quantum supremacy as a demonstrative example to encourage development and reex-

Exec. Order No. 13587 § 5.2, 76 Fed. Reg. 63,811, 63,813 (2011); Exec. Order No. 13636, 78 Fed. Reg. 11,739 (2013); Exec. Order No. 13800 § 1(C), 82 Fed. Reg. 22,391, 22,392 (2017); OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB CIRCULAR NO. A-130 (2016); NAT'L INST. STANDARDS & TECH., NIST SP 800-37 REV. 2, RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS: A SYSTEM LIFE CYCLE APPROACH FOR SECURITY AND PRIVACY (2018); NAT'L INST. STANDARDS & TECH., NIST SP 800-53 REV. 4, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (2015); COMM. ON NAT'L SEC. SYS., CNSSP NO. 21, NATIONAL CYBERSECURITY POLICY ON ENTERPRISE ARCHITECTURE FRAMEWORKS FOR NATIONAL SECURITY SYSTEMS (2016); COMM. ON NAT'L SEC. SYS., CNSSP NO. 25, NATIONAL POLICY FOR PUBLIC KEY INFRASTRUCTURE IN NATIONAL SECURITY SYSTEMS (2017); COMM. ON NAT'L SEC. SYS., CNSSP NO. 30, CRYPTOGRAPHIC KEY PROTECTION (2017); COMM. ON NAT'L SEC. SYS., CNSSD NO. 506, NATIONAL DIRECTIVE TO IMPLEMENT PUBLIC KEY INFRASTRUCTURE ON SECRET NETWORKS (2019); COMM. ON NAT'L SEC. SYS., CNSSI NO. 1253, SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS (2014); COMM. ON NAT'L SEC. SYS., CNSSI NO. 1300, (U) INSTRUCTION FOR NATIONAL SECURITY SYSTEMS PUBLIC KEY INFRASTRUCTURE X.509 CERTIFICATE POLICY UNDER CNSS POLICY NO. 25 (2014); for Department of Defense organizations, DEP'T OF DEF., INSTRUCTION 8500.01, CYBERSECURITY (2014) [hereinafter CYBERSECURITY]; DEP'T OF DEF., INSTRUCTION 8320.01, INFORMATION TECHNOLOGY STANDARDS IN THE DOD (2013); DEP'T OF DEF., INSTRUCTION 8551.01, PORTS, PROTOCOLS, AND SERVICES MANAGEMENT (PPSM) (2017); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, CJCSI 6211.02D, DEFENSE INFORMATION SYSTEMS NETWORK (DISN) RESPONSIBILITIES, at D-10–11 (2012), https://www.jcs.mil/Portals/36/Documents/Library/Instructions/6211_02a.pdf?ver=2016-02-05-175050-653; CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION, CJCSI 6510.01F, INFORMATION ASSURANCE (IA) AND SUPPORT TO COMPUTER NETWORK DEFENSE (CND) (2011). This list is not all-inclusive. The author realizes there are a myriad of risk management framework regimes. The author, however, coins the term "legal risk management framework (LRMF)" to discuss the collection of legal regimes imposing obligations on agencies and officials to protect information systems with appropriate tactics, techniques, procedures, and qualitative decision-making cycles.

amination of the LRMF. Beginning with Part II, this Article provides an overview of quantum computing, national security systems, concepts of network security, and the threats posed to current encryption standards that protect national security systems. Part III summarizes and paraphrases the LRMF. Part IV provides a short description of the term "resiliency" as related to cybersecurity. Part V provides recommendations to assist thinking about the LRMF and how to achieve resiliency. Lastly, Part VI offers concluding remarks. This Article is not meant to be exhaustive. It strives to encourage a conversation about how the industry can better protect national security systems from emerging and threatening technologies.

II. QUANTUM, NETWORK SECURITY, AND NATIONAL SECURITY SYSTEMS: DEMONSTRABLE EVIDENCE

A. Quantum Supremacy, Quantum Computing, and Classical Computing

Quantum Supremacy is defined generally as the ability of a quantum computer to successfully solve a problem that no classical computer can solve.[12] As related to this Article, it includes the ability to solve encryption that no classical computer can overcome.[13] Quantum Supremacy is thought to occur once a quantum computer is able to continuously entangle fifty qubits. Google was able to entangle fifty-three qubits. It is easy to see why their claim to quantum supremacy carries with it a level of validity.[14] The ability to entangle these qubit promises potential uses such as machine learning,[15] optimization,[16] and future factoring of complex encryption algorithms currently used for information security purposes.[17] These functions will be performed at rates far faster than classical computers.[18]

Stated simply, quantum computing is the process by which computers use principles of quantum physics, mechanics, and information science for

12. Arthur Herman & Idalia Friedson, *Quantum Computing: How to Address the National Security Risk*, HUDSON INST. 3, 3–9 (Aug. 2018), https://www.quintessencelabs.com/wp-content/uploads/2018/09/Quantum-National-Security-Risk.pdf; *see* Ali, *supra* note 4, at 12.

13. Herman & Friedson, *supra* note 12, at 3; Ali, *supra* note 4, at 10–11.

14. Herman & Friedson, *supra* note 12, at 7.

15. *See* Ali, *supra* note 4, at 15 (discussing the ability to train artificial intelligence through the creation of more potent algorithms by using massive datasets, adversarial competition, micromanagement, and other corrective measures).

16. *See* Nikolaj Moll et al., *Quantum Optimization Using Variational Algorithms on Near-Term Quantum Devices*, QUANTUM SCI. & TECH. 1, 3 (July 2018). The authors point out that ability to find the best solution to a problem from triage of options.

17. Herman & Friedson, *supra* note 12, at 7–8; Ali, *supra* note 4, at 11.

18. Ali, *supra* note 4, at 7–9.

increased computational power and speed.[19] By using the underlying foundation of quantum mechanics—"information, probabilities, and observables, and how they relate to each other"—quantum computers can perform simultaneous calculations by measuring physical photons, electrons, or atom nuclei of data.[20] These simultaneous states are captured in information known as *qubits*.[21] Qubits are physical in nature and continuous.[22] Thus, any measurement captures a value based upon a distributed probability at the time of measurement.[23] Qubits are quantum computing's version of *bits* used by classical computers, literally the "ones and zeros" [1, 0] for coding.[24] They can be harnessed in a two-dimensional forms known as *superposition*, where information exists in multiple states at once by a processes of intimate correlation and connection (*entanglement*).[25] This means that they are not limited to binary states of coding used by classical computers (0 or 1), but instead, can be combinations thereof (for example, [0, 1], [00], [01], [10], etc.).[26] In theory, there are infinite numbers and possibilities for these values.[27]

In contrast, classical computing uses binary and linear states of logic code.[28] These binary and linear states are comprised of electrons represented by either one or zero (1, 0).[29] They do not exist simultaneously.[30] These binary and linear logic codes may be unsatisfying to quench today's thirst for more computational power and speed. The principle of "Moore's law" dictates that binary and linear logics' computing power doubles every year, but eventually, these speeds will have trouble keeping up with demand.[31] It appears clear how and why quantum computing is different: (1) from a techni-

19. *Id.* at 8.

20. *Id.*; *see also* SCOTT AARONSON, QUANTUM COMPUTING SINCE DEMOCRITUS 11 (2013) ("From [my] perspective, [quantum mechanics] it's about information and probabilities and observables, and how they relate to each other. [It] is what you would inevitably come up with if you started with probability theory, and then said, let's try to generalize it so that the numbers we used to call 'probabilities' can be negative numbers.").

21. Ali, *supra* note 4, at 8; AARONSON, *supra* note 20.

22. Ali, *supra* note 4, at 8; AARONSON, *supra* note 20.

23. Ali, *supra* note 4, at 8; AARONSON, *supra* note 20.

24. Ali, *supra* note 4, at 9.

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

30. Ali, *supra* note 4, at 9.

31. *Id.* at 10.

cal point-of-view, it adds a new dimension to *bits*; and (2) it may provide the new rates of computational power in speed to meet increasing demand.

B. National Security Systems, Encryption Standards, and Network Security

Where these two separate computing methodologies clash is in their relation to NSSs which hold valuable information, and the encryption standards that protect these systems. NSSs are defined by statute as:

> [A]ny information system . . . used or operated by an agency or by contractor of an agency, or other organization on behalf of an agency [whose] function, operation, or use . . . involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon system; or . . . is critical to the direct fulfillment of military or intelligence missions.[32]

It does not include systems meant for administrative or business applications such as employee payroll, finance, logistics, or personnel management.[33] Given the clear and unambiguous language defined by this statutory definition, the systems of concern here, military and intelligence systems, fit neatly within this statutory definition.[34] These NSSs are required to implement a variety of encryption standards for the protection of data they hold.[35] Depending on the specific system, more stringent requirements are warranted.

Encryption protects data held in NSSs and is defined as the process of converting original data into a chaotic and unusable form to protect it from unauthorized parties—it is needed because a NSS will contain the same components of basic computer networks, albeit specialized for a national security organization.[36] These components include nodes, hosts, connection protocols, firewalls, boundary networks, workstations, servers, switches, routers, and many other components.[37] Each one of these aspects to a system permit identification, communication, and appropriate filtering of ingress and egress

32. 44 U.S.C. § 3552(b)(6)(A)-(B). The author would argue that systems that contain *sensitive* personnel, finance, and personnel management systems would fit neatly in this definition, i.e. covered intelligence agents, etc.

33. *Id.*

34. *See* VALERIE C. BRANNON, CONG. RSCH. SERV., R45153, STATUTORY INTERPRETATION: THEORIES, TOOLS, AND TRENDS 19–28 (2018), https://crsreports.congress.gov/product/pdf/R/R45153.

35. *See, e.g.*, sources cited *supra* note 11.

36. *See* J. MICHAEL STEWART, NETWORK SECURITY, FIREWALLS, AND VPNS 24–39 (2d ed. 2014).

37. *Id.*

traffic within a network.[38] Malicious actors take advantage of each component by using a variety of tactics, techniques, and procedures to impact confidentiality, integrity, and availability of the resources an organization pulls from a NSS, all goals in which cybersecurity seeks to achieve.[39]

To date, the most secured, publicly available encryption standards for classical computing involve uses of large mathematical operations known as "public-key" cryptology which scrambles information until it is unlocked.[40] This form of encryption is used to protect NSSs. This cryptologic process uses a two-staged, asymmetrical protocol that splits access between parties before information is readable by demanding large integer factoring.[41] Information may not be read until one party generates a private key to decrypt information, sends it to another party, and the receiving party uses the public key containing the answer to the large integer.[42] The public key is generally only available to a trusted party who is authorized to factor the large integer.[43] Until the large integer is factored, information remains unreadable.[44] This process is extremely reliable given that classical computing attempts to forcibly break this two-staged process could take years.[45] Depending on time constraints, this is an unreasonable length of time if one party's intent is to access the information to quickly gain a competitive edge.

Quantum supremacy changes this unreasonable amount of time to forcibly break the aforementioned encryption standard.[46] The increased computing power and speed will dramatically reduce the time needed to factor large integer.[47] Given that qubits exist in simultaneous states, it may simultaneously generate every possible answer to a large integer, as well as alternative answers at increasing speeds.[48] What used to take years, may now take seconds.[49] This will render current encryption standards moot.

38. *Id.*

39. *Id.* at 20–39.

40. Ali, *supra* note 4, at 10.

41. *Id.*

42. *Id.*

43. *Id.* at 10–11.

44. *Id.*

45. *Id.*

46. *See* Keith Crane et al., *Assessment of the Future Economic Impact of Quantum Information Science*, IDA Sci. & Tech. Pol'y Inst. 1, 33–34 (2017), https://www.ida.org/-/media/feature/publications/a/as/assessment-of-the-future-economic-impact-of-quantum-information-science/p-8567.ashx.

47. *Id.*

48. *Id.*

49. *Id.*

One can imagine serious impacts such as an adversary accessing decades worth of intelligence information; military operational plans; covert and clandestine operational information; or even secret personnel files. Moreover, if combined with developing technologies and methodologies, such as artificial intelligence[50] and machine learning,[51] for more rapid decision-making cycles in its employment, it is clear to see that the security implications are astounding.

C. The Importance of Understanding Network Security & the Seven Domains of Information Technology Infrastructure

To conceptualize the issue of encryption and the impacts of Quantum Supremacy, one must consider the concept of network security as the landscape in which these impacts occur.

Network Security can be defined as "the control of unwanted intrusion into, use of, or damage to communications on [an] organization's computer network."[52] At a basic level, this includes a host of activities to include monitoring ones network for abuses and hackers, blocking unapproved transmissions, and responding to issues of operability.[53] For NSSs, or any computer system for that matter, the goal of network monitoring is to ensure the access to resources for those privileged to use the systems while denying this access to those unapproved to use the network.[54]

One starts network monitoring by determining exactly what they are trying to protect—here, national security systems.[55] This includes the physical infrastructure, the data and code that runs the system, and the people that use the system.[56] Notwithstanding particulars of a computer network, at minimum, it includes seven layers: (1) the User domain; (2) Workstation domain; (3) Local Area Network (LAN) domain; (4) LAN-to-Wide Area Network (L-

50. *See* Salahudin Ali, *Cybersecurity Support of Insider Threat Operations: DoD Regulation and Constitutional Compliance*, 30 GEO. MASON U. C.R.L.J. 1, 15–16 (2019) (mentioning that AI can generally be considered algorithmic ability which mimics human critical thinking based on observations and decisions an agent makes to solve complex problems presented by observables).

51. *See* Ali, *supra* note 4, at 15–16 (mentioning process by which artificial intelligence trains on massive pre-programmed data sets that are matched via algorithm through a variety of methods such as adversarial competition, micromanagement, and other corrective measures to create better algorithms for future decision making).

52. STEWART, *supra* note 36, at 4.

53. *Id.*

54. *Id.*

55. *Id.* at 7.

56. *Id.*

WAN) domain; (5) Remote Access domain; (6) WAN domain; and (7) the System/Application domain.[57]

The User domain includes people who access a computer network.[58] The workstation domain includes hardware such as desktop computers, laptops, and other devices; this layer is responsible for the transmission of raw data.[59] The LAN domain includes the hardware and software used to support the workstation's connectivity to the rest of the network.[60] The L-WAN domain refers to the interworking and interconnecting points between the LAN and WAN network, i.e. the point of entry and departure from an intranet and internet.[61] The Remote Access domain refers to the procedures which authenticate and authorized remote connection to an IT network.[62] The WAN domain refers to the remote locations of routers, switches, firewalls, and other gear that provide bandwidth for connectivity; these are usually managed by internet service providers (ISPs).[63] Lastly, the System and Application Domain refers to hardware and software operating systems that house data.[64]

The above assists in conceptualizing the landscape to promote a strategic philosophy of cybersecurity. End-goals of network security ensure confidentiality of resources; protecting the integrity of data; ensuring availability of data; ensuring privacy of personal protected data; access control; effective monitoring for violations of policy and use within a network; and ensuring the system supports the mission of an organization.[65]

Trust is key in the process of network monitoring.[66] It demands confidence that users will abide by appropriate user policy and rules established by a computer network's administrator.[67] From a legal standpoint, this is done through user agreements or other terms-of-use; from a technical standpoint, this is done through certificates that verify that a person is a trusted (good) user of a computer network.[68] A user interacts with a main server

57. *Id.* at 9–12.

58. STEWART, *supra* note 36, at 9.

59. *Id.*; *see also Goals of Networking*, N.Y.U. COMPUT. SCI. DEP'T., https://cs.nyu.edu/courses/spring00/V22.0480-002/class01.html (last visited Apr. 5, 2021).

60. STEWART, *supra* note 36, at 9.

61. *Id.*

62. *Id.* at 9, 10.

63. *Id.*

64. *Id.*

65. *Id.*

66. STEWART, *supra* note 36, at 6–7.

67. *Id.*

68. *Id.*

which vets a user's credentials, ensuring they are who they say they are, and gives users access (permission or privileges) to use resources within the computer network.[69] The result is that confidentiality, integrity, and availability of a computer networks resources are maintained.[70]

These seven domains and the security goals thereof align with the goals of encryption (recognizing that encryption is a subcomponent of cryptology) which are the privacy, authenticity, and integrity of data.[71] As mentioned above, encryption is a process which protects the data that is transferred within and from the seven domains.[72] It ensures, through overlapping goals, that network security actually works.[73] As related to Quantum Supremacy, anticipation and the ability to absorb such an impact must be taken seriously. Quantum Supremacy disrupts these goals in ways previously not considered.[74]

III. THE LEGAL RISK MANAGEMENT FRAMEWORK

Requirements from a legal perspective are important to agencies and the officials that run them. Every agency—especially head and lead officials—should be familiar with statutory and regulatory authority that drives decision making and action. Indeed, statutes and regulation are important because they declare legal duties and authoritative direction, as well as impose levels of legal sufficiency in accomplishing the overall mission.[75] The LRMF adopts standards required by federal statute, executive branch regulation, and policy to address risks posed to its information systems.[76]

Language from the LRMF eventually makes its way to written policy as underlying legal authority. For example, Department Defense Instruction 8500.01 and 8510.01 serve as the overall cybersecurity policy and lay the framework for cybersecurity in the Department of Defense.[77] The existence of a written cybersecurity policy is important because it encapsulates the

69. *Id.*

70. *Id.*

71. Mindi McDowell, *Security Tips (ST04-019): Understanding Encryption*, Cybersecurity Infrastructure Sec. Agency, https://us-cert.cisa.gov/ncas/tips/ST04-019 (last modified Sept. 27, 2019).

72. *Id.*; *see also* Ali, *supra* note 4, at 10–11.

73. McDowell, *supra* note 71; Ali, *supra* note 4, at 10–11.

74. *See supra* text accompanying notes 47–52.

75. Jules Coleman & Scott Shapiro, The Oxford Handbook of Jurisprudence & Philosophy of Law 267–68 (Jules L. Coleman et al. eds., 2002).

76. Risk Management Framework, *supra* note 9.

77. *Id.*; Cybersecurity, *supra* note 11.

LRMF discussed above, as well as its goals.[78] Written policy guides management and users toward those goals and serves a reference point for the collective of law, regulation, and organizational cybersecurity policy, ensuring a common understanding and the availability to conduct quality assurance assessments about the success of a cybersecurity program.[79]

The LRMF is unique in addressing cybersecurity because networks exist in the larger internet.[80] Since its advent, the internet has primarily been a space of norms and not legal governance.[81] Originally developed simultaneously by the Department of Defense and university researchers during the 1960s through the 1980s, the internet moved toward privatization at the end of the 20th century.[82] Security was not the primary concern for this invention.[83] The concept was a new, transformational way for like-minded individ-

78. *See* STEWART, *supra* note 36, at 11. To note, this is distinguishable from *Technical Policy* for IT. Technical Policy enforces organizational written policy through configurational and control procedures which map to organizational written policy. For example, a written policy may provide that a password be "strong." Through Technical Policy, configuration may demand that passwords which do not include a combination of numbers, letters, and symbolisms are not allowed. Moreover, a written organizational policy may require that personal identifiable information (PII) must be protected. The Technical Policy will provide configuration such as a specific type of encryption and digital signature before such information can traffic a network. Thus, through *technical* controls, written policy is enforced. For purposes of this Article, these Technical Policies that enforce written policy, should be mapped to underlying legal obligations. *See Computer Security Resource Center: Technical Controls*, NAT'L INST. STANDARDS TECH., https://csrc.nist.gov/glossary/term/Technical_Controls (last visited Apr. 5, 2021); *see also The Key Difference Between Policy vs. Procedures*, COMPLIANCEBRIDGE, https://compliancebridge.com/policy-vs-procedures/ (last visited Apr. 5, 2021).

79. *See* STEWART, *supra* note 36, at 11; *Computer Security Resource Center: Technical Controls*, *supra* note 78; *The Key Difference Between Policy v. Procedures*, *supra* note 78.

80. *See* STEWART, *supra* note 36, at 24; *Computer Security Resource Center: Technical Controls*, *supra* note 78; *The Key Difference Between Policy v. Procedures*, *supra* note 78.

81. *See* Philip J. Greene, *Legal Foundations of the Internet; Technical Management and Coordination; and the Standards and Protocol Setting Process and Protocol Setting Processes; Identity and Description of Key Entities in Internet Governance*, VICTORIA UNIV. OF WELLINGTON 1 (Nov. 6, 2007), http://old.internetnz.net.nz/issues/archive/other/governance.pdf.

82. *Id.* at 2–11.

83. Ali, *supra* note 4, at 6 ("[C]yberspace quickly emerged as an academic and consumer enterprise focused on the ease and efficiency of communicating information, in direct contrast to the security of information. The current model for creating programs and applications that later fix vulnerabilities—"patch-

uals to communicate their ideas.[84] Private organizations developed sets of rules and protocols for the internet's working to ensure smooth communication and access to the many independent networks, creating a "web," or more appropriately, a "world-wide web."[85] This web of networks includes millions of pieces of hardware, software, and individual users that are, in theory, holistically connected.[86] The advent of malicious actors, however, always pacing ahead of government attempts to create regulation of the internet, quickly took advantage of the lack of security awareness regarding national security systems.[87] Therefore, the LRMF framework for NSSs is best thought of as addressing the very nature of the internet as a holistic threat given the circumstances.

Collectively, the LRMF is large and nuanced. But it is possible to draw certain overall legal requirements for agency officials. Having its origins within legislation such as the Clinger-Cohen Act,[88] Federal Information Security Management Act of 2002,[89] and the Federal Information Security

ing," a software update that temporarily fixes an existing vulnerability before the full release of entirely new software—is ill-suited for national defense.").

84. *Id.*

85. *See* Greene, *supra* note 81, at 2–11.

86. *See* STEWART, *supra* note 36, at 24.

87. Historically significant developments of malicious actors can be traced from the 1970s until recent. Notable early developments include the "Vampire Worm" developed by John Hupp and John Shoch of Xero's Palo Alto Research Center (which shut down computers at night), as well as their "Town Crier Worm" that moved shared announcement throughout a network. Another example is offered by the US Leasing hacks tied to Kevin Mitnick in 1980 that slowed the company's computers and left vulgar messages. Moreover, the MORRIS WORM offers an early example of hacking on a massive scale, exploiting vulnerabilities in UNIX code, freezing private and government computers around the United States. Lastly, SOLAR SUNRISE and MOONLIGHT MAZE were attacks on U.S. military systems attributed to American teenagers and Russian operatives, separately. *See, e.g.*, JOHN P. CARLIN, DAWN OF THE CODE WAR 79–128 (2018). Attempts have been made to address these early hacking attempts. Legislation such as the Computer Fraud and Abuse Act, 10 U.S.C. § 1030, *et seq.*; Communication Decency Act of 1996, 47 U.S.C. § 230; and Digital Millennium Copyright Act, Pub. L. No. 105-304, all offer examples of addressing hacking, intellectual property abuse and theft, and circumvention of encryption (discussion of these legislation is beyond the scope of this Article).

88. Clinger-Cohen Act for Fiscal Year 1996, Pub. L. No. 104-106, §§ 4001–4402, 5001–5703, 110 Stat. 186, 642–703 (1996).

89. Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002).

Modernization Act of 2014[90] (and many more), a framework was developed to ensure efficient, administrative practices for procuring and implementing information technology into government systems.[91] These statutes created the position of Chief Information Officer for federal agencies and empowered them to advise, create, and enforce cybersecurity standards—primarily, their responsibility is assuring the "availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential."[92] All elements of network security are discussed above.[93]

As threats of malicious cyber activity increased, focus began to move toward that of an operational framework, providing more discretion and decision-making capacity for military commanders within a Goldwater-Nichols Act framework.[94] This framework reorganized the chain-of-command of military organization charged with conducting warfare.[95] This new framework essentially placed cyber risk management in the hands of those who are in contact with adversaries by recognizing that cybersecurity is part of military operational warfare.[96] This move hit its zenith with the elevation and declaration of cyberspace as an operational domain, warranting military commander leadership in the decision-making process.[97] However, the original LRMF did not disappear. It remains in place and must be considered in the overall IT planning framework. As with most legislation, internal regulation followed and continues to develop as new threats emerge.[98]

Moving the management of cyberspace to the hands of military commanders signaled a cultural shift that must be noted. As management moves towards those who govern the operational domain of cyberspace, a mere risk-adverse approach may not be appropriate. Strategically, commanders seek authority and courses-of-action that can withstand the impact of brute-force

90. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

91. *See* Ali, *supra* note 4, at 15–16; STEWART, *supra* note 36, at 4.

92. 10 U.S.C. §§ 2223(a)–(b), 2224(b) (2004).

93. *See supra* Part II.C.

94. Memorandum from the Sec'y of Defense on the Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations for Sec'ys of the Military Dep'ts (June 23, 2009), https://fas.org/irp/doddir/dod/secdef-cyber.pdf [hereinafter Sec'y of Defense Memorandum]; *see also* 10 U.S.C. §§ 161–166b, 167b (2018).

95. Sec'y of Defense Memorandum, *supra* note 94; 10 U.S.C. §§ 161–166b, 167b.

96. DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

97. Sec'y of Defense Memorandum, *supra* note 94; 10 U.S.C. §§ 161–166b, 167b.

98. *See* sources cited *supra* note 11.

actions. The expectation is that systems will be used in military actions and thus will become targets to adversaries.[99] A mere risk management approach fits an approach by agency officials charged with functionality (i.e., does the system work?).[100] The difference in nomenclature—here, "operability"—is key. As NSSs become part of the military operational domain of cyberspace, operability is more appropriately defined by its systems resiliency, as opposed to its initial functionality. Thus, old standards may need revision in light of this new reality.

Risk to NSSs is managed through a set of technical policy through control measures and categorization; for example, discerning whether specific tactics, techniques, and procedures (TTPs) run a or High, Medium, Low risk if implemented.[101] These control measures and categorizations of risk allow organizations to determine what risk levels are acceptable to an agency based upon its unique mission, operational culture, and leadership philosophy. It also allows discretion as to what mechanisms and control measures can assist in managing such risk.[102] Software, or devices that use software to connect to national security systems, must comply with the information security standards issued and adopted by national security and intelligence agencies. These standards include having an appropriate security screening and preauthorization by an Authorizing Official—a person authorized to approve software and hardware for connection to a national security system.[103]

For NSSs, the LRMF requires that agencies develop, maintain, and implement sound, secure, and integrated information technology architecture.[104] Moreover, it requires that agency officials provide information security protections for NSSs and commensurate with the risk and magnitude of harm by complying with information standards and guidelines provided by law and

99. *See, e.g.*, U.S. MARINE CORPS, MARINE CORPS DOCTRINAL PUBLICATION 1-3 TACTICS, at 81–88 (July 30, 1997), https://www.marines.mil/Portals/1/Publications/MCDP%201-3%20Tactics.pdf. This maneuver warfare concept is captured in the concept of *adaption*, prevalent in the United States Marine Corps—an expeditionary warfighting organization.

100. *See* U.S. Dep't of Energy, *Recovery Act: Standards, Interoperability, and Cybersecurity*, SMARTGRID.GOV, https://www.smartgrid.gov/recovery_act/overview/standards_interoperability_and_cyber_security.html (last visited Apr. 6, 2021) ("Interoperability is defined as the capability of two or more networks, systems, devices, applications, or components to share and readily use information securely and effectively with little or no inconvenience to the user.").

101. *See* COMM. ON NAT'L SEC. SYS., CNSSP NO. 17, POLICY ON WIRELESS SYSTEMS (2014); COMM. ON NAT'L SEC. SYS., CNSSI NO. 1253, SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS (2014).

102. *See* sources cited *supra* note 11.

103. *See* 40 U.S.C. § 11331 (2002); 44 U.S.C. § 3554 (2018); 10 U.S.C. §§ 2224–2224a (2004).

104. *See* sources cited *supra* note 11.

Presidential direction.[105] This can include certain periodic testing of the impacts of unauthorized access and disclosure of information, qualifications of personnel who operate such a system, and implementation of automated detection systems.[106] Importantly, the existing LRMF is not overly prescriptive and leaves wide discretion to agencies and their officials, allowing a level of flexibility. The paradox being that the LRMF may be too focused on technical aspects to accomplish requirements as to its overall intent opposed to prescriptive requirements that require agencies and their officials to make decisions.

Through executive order, NSSs are required to follow those standards developed by the National Institute of Standards and Technology (NIST), as implemented through several Committee on National Security System rules and regulation, to manage agency cybersecurity risk.[107] These regulations provide that agency officials will be "held accountable for implementing risk management measures" and for "ensuring that cybersecurity risk management process is aligned with strategic [and] operational" processes in accordance with the statute.[108] Plans are expected to include strategies, operational, and budgetary considerations that inform choices; accepted risk for unmitigated vulnerabilities; and even plans to deal with "botnets" and other automated, distributed threats.[109] This is done through a process of categorizing information systems (classified, investigative, medical information, etc.), and then select security controls.[110] For encryption, this includes the use of public-key infrastructure mentioned above and consists of asymmetrical encryption which is currently the strongest encryption for classical computing.[111]

105. *Id.*; *see also* Exec. Order No. 13800 §1(a), 82 Fed. Reg. 22,391, 22,392 (2017).

106. *See* sources cited *supra* note 11; *see also* Exec. Order No. 13800 § 1(c), 82 Fed. Reg. at 22,392.

107. *See* sources cited *supra* note 11; *see also* Exec. Order No. 13800 § 1(c)(2)(ii); 82 Fed. Reg. at 22,392; Exec. Order No. 13587 § 5.2; 76 C.F.R. 63, 811, 63, 813 (2011).

108. Exec. Order No. 13800 § (1)(c)(i) 82 Fed. Reg. at 22,392.

109. *Id.* § 2.

110. *See* sources cited *supra* note 11.

111. *See* NAT'L INST. STANDARDS & TECH., NIST SP 800-37 REV. 2, RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS: A SYSTEM LIFE CYCLE APPROACH FOR SECURITY AND PRIVACY (2018); NAT'L INST. STANDARDS & TECH., NIST SP 800-53 REV. 4, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (2015); CNSSP NO. 21, NATIONAL CYBERSECURITY POLICY ON ENTERPRISE ARCHITECTURE FRAMEWORKS FOR NATIONAL SECURITY SYSTEMS (2016); COMM. ON NAT'L SEC. SYS., CNSSP NO. 25, NATIONAL POLICY FOR PUBLIC KEY INFRASTRUCTURE IN NATIONAL SECURITY SYSTEMS (2017); COMM. ON NAT'L SEC. SYS., CNSSP NO. 30, CRYPTOGRAPHIC KEY PROTECTION (2017); COMM. ON NAT'L SEC. SYS., CNSSD NO. 506, NATIONAL DIRECTIVE TO IMPLEMENT PUBLIC KEY

What may be missing are key points in law and regulation that assume NSSs will be compromised and the mandate that contingency plans be built with this expectation in-mind. Instead of managing risk from a technical perspective, or as normative behavior, focus is more appropriately aimed at managing and adapting to the *impacts* of such risk through broader concepts of what makes a system resilient as a legal duty.

IV. RESILIENCY

Richard Clarke notes in his book, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*,[112] that resiliency is the "capacity of any entity . . . to prepare for disruptions, to recover from shocks and stresses, and to adapt and grow from a disruptive experience."[113] It is hard sought to find a better statement than that which accurately captures this concept. The most important aspect of this concept is not just the ability to return or withstand trauma but the ability to learn from it through adaptation.

Resiliency, with foundations in the study of social ecological systems (SES), requires thinking that promotes adaptability and transformability.[114] Adaptability assists in adjusting to circumstances and influences outcomes.[115] Transformability assists in learning to survive in a changed environment.[116] This is important because SESs are thought to exist within certain critical thresholds which allow for survivability.[117] If a SES cannot cope with external drivers that cause perturbation, the critical threshold will be crossed and make the SES too unstable for existence.[118] Through resiliency, new stable environments may be created after the initial shock of external factors, allowing for survival within a new, stable environment within the critical threshold.[119]

INFRASTRUCTURE ON SECRET NETWORKS (2019); COMM. ON NAT'L SEC. SYS., CNSSI NO. 1253, SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS (2014); COMM. ON NAT'L SEC. SYS., CNSSI NO. 1300, (U) INSTRUCTION FOR NATIONAL SECURITY SYSTEMS PUBLIC KEY INFRASTRUCTURE X.509 CERTIFICATE POLICY UNDER CNSS POLICY NO. 25 (2014); *see also* Ali, *supra* note 4, at 10.

112. CLARKE & KNAKE, *supra* note 2.

113. *Id.* at 15.

114. *See* Carl Folke et al., *Resilience Thinking: Integrating Resilience, Adaptability and Transformability*, 4 ECOLOGY & SOC'Y 1, 2–4 (2010), http://www.ecologyandsociety.org/vol15/iss4/art20/.

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

Adaption and transformability are not to be applied narrowly nor lackadaisically. This change must be deliberate and applied more generally.[120] External drivers are unpredictable (like IT environments). Thus, anticipation of the unknown and preparation through learned behavior is key to keeping environments within critical thresholds.[121] This set of thinking allows for a new trajectory despite impacts by external factors.[122] For IT networks, particularly NSSs, this is done through a strategy defined by a written policy.[123] Strategy requires that one not only continuously seeks to reduce risk and vulnerabilities but also create processes and procedures to limit damage done to systems. Essentially, one grows from the experience through appropriate risk management—especially when it is a requirement by law.

This concept of resiliency, and the analogy of SESs is uniquely suited for the LRMF because managing risk involves more than mere mitigation.[124] Like SESs, NSSs exist in a novel environment where external drivers can impact them beyond their critical threshold of operability. It is not a question whether a data system will be compromised but when it will be compromised.

What occurs after one mitigates damage is key. Agencies and officials need guidance. Indeed, they expect it, bureaucracy works no other way. Some corporations have adopted this concept through policy and have flown under the radar considering the pervasiveness of today's cybersecurity crises (known as the "dog that does not bark.").[125] For example, during the "NotPetya" cyber operations in Ukraine, where many international businesses are located, many of these companies did not appear to be operationally impacted.[126] Cybersecurity experts contribute this to these companies' resiliency framework which allowed sound risk management and cybersecurity practice.[127] In other words, sound cybersecurity practices allow an IT network's trajectory toward a new zone of stability without crossing the critical threshold of inoperability.

120. Folke et al., *supra* note 114, at 3.

121. *Id.*

122. *Id.*

123. *See supra* Part III.

124. *See* sources cited *supra* note 11.

125. CLARKE & KNAKE, *supra* note 2, at 29, 33–35; *see also* The CyberWire Daily, *Ep 28: The Fifth Domain Coauthor Richard A. Clarke*, CYBERWIRE, at 16:37 (July 21, 2019), https://www.thecyberwire.com/podcasts/cw-podcasts-special-2019-the-fifth-domain-coauthor-richard-a-clarke.html.

126. CLARKE & KNAKE, *supra* note 2, at 29. These companies included the likes of Hyatt Hotels, Johnson & Johnson, Boeing, and John Deere, respectively.

127. *Id.* at 29–47.

Those charged with creating standards for NSSs should do the same. It is only through this mechanism that this concept of resiliency crosses the threshold of being merely aspiration and into something more real.

V. RECOMMENDATIONS

This gap can be covered with recommended additions to the LRMF. The below recommendations are not meant to be restrictive or draconian. Instead, the recommendations seek to change the way agencies think about the LRMF as a legal regime considering new, advanced computing technologies—here, quantum supremacy. The below list is also not meant to be exhaustive. It may, however, start a conversation that leads to the ability to operate NSSs on a level of continuity needed to achieve resiliency through legal mandate.

A. LRMF Recommendations

1. Near Term Changes to Encryption Standard

The LRMF should provide that agencies maintain a plan to deal with the impacts of quantum supremacy or other post-Public Key Infrastructure (PKI) resistant computing. For example, this could include the adoption of post-quantum cryptology in the form of quantum resistant algorithms (QRAs); quantum random-number generators (QRNGs); or lattice-based cryptology.[128] QRAs use *really* difficult and large integers built to withstand impacts of quantum computer factoring.[129] QRNGs use truly random numbers generated by naturally occurring randomness (measuring of solar flares, for example).[130] QRNGs may be useful to stale or prevent quantum supremacy's ability to overwhelm classical encryption such as PKI (NIST has already begun this process).[131] Lastly, Lattice based cryptology uses constructions of algorithmic protocols used to build cryptology by relating their construction to proofs of extremely hard math problems.[132] Through a process of spaced grids of evenly distributed but infinite number of vectors that enable the connection of non-linear coordinates—this presents an infinite number of possible coordinates.[133] This type of encryption, if mandated by law, provides the level of risk management to remain operable in the face of quantum supremacy.

128. Ali, *supra* note 4, at 42–43.

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

2. The LRMF Should Require Agencies and Agency Officials to Continue to Engage with the Private Sector for Expertise on Emerging Computer Threats on a Cerebral Level Outside of the Procurement Process

This will depend on strict compliance with current Ethics and Standards of Practice regulation governing agencies and officials.[134] The National Defense Authorization Acts of 2020[135] and 2019[136] provide authorizations in U.S.C. Section 2358 of Title 10.[137] Collectively, they require "the Secretary of Defense [to] carry out a quantum information science and technology research and development program."[138] Additionally, the Secretary of Defense must now "develop plans for reducing the risk of cybersecurity threats posed by quantum information science technology."[139] This is accomplished by coordinating research and development cooperation with "private entities and international entities."[140] Cooperation and coordination can be done in many ways, but outside the procurement process, this can be accomplished through communities of practice or a number of public-private interest groups.[141] The aforementioned acts are an encouraging sign for the LRMF in relation to Quantum Supremacy. Although, the language *should* read that the Secretary shall at least demonstrate that they have engaged with private entities and international entities to develop plans to not only reduce risk, but to ensure operability from the impacts of such risk: this becomes a statutory requirement for resiliency.

3. The LRMF Should Require More Stringent Standards Applied to the Private Sector to Show Their Products Add Value to NSSs' Cybersecurity

Building from recommendation two, a private sector company should be able to point directly to some sort of matrix to show how the product contributes to a control measures and security standards, and not just another layer

134. *See, e.g.*, 5 C.F.R. § 2635.101(b); SEC'Y OF DEFENSE, DOD 5500.7-R, JOINT ETHICS REGULATION (1993) (these regulations also adopt contract integrity guidelines).

135. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 220, 133 Stat. 1198 (Dec. 20, 2019).

136. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, § 234, 132 Stat. 1636 (Aug. 13, 2018).

137. 10 U.S.C. § 2358 (2017).

138. *See supra* notes 134–137 and accompanying text.

139. *Id.*

140. *Id.*

141. *Id.*

atop of an existing landscape.[142] This can be anything from showing more advanced forms of coding, showing the ability of agencies to modify products (like in cloud computing)[143] or requiring access to lab results (failures and successful test results).[144] At this point, an agency would have total awareness of the product they are purchasing, and the private sector would be forced to develop products focused on their qualitative and quantitative values.

4. The LRMF Should Require Intelligence and Operational-Based Defenses for NSSs. This is Often Captured in Cybersecurity Nomenclature as a "Kill-Chain"

This is an expansion from many different decision-making cycles such as Colonel Boyd's "OODA-LOOP (observe, orient, decide, Act [repeat])" and the Joint Improvised Explosive Device Defeat Organization's process to get "left of boom" from roadside bombs (reconnaissance, weaponization, delivery, exploitation, installation, command & control, and actions).[145] The benefit of this process is that it allows an agency to identify, detect, and stop a malicious actor at any stage of their operation because each piece of a malicious actor's attack is identified.[146] If a plan is developed to disrupt any of these pieces to a decision-making cycle, a national security system may remain resilient due to the ability to select control measures and contingency plan for each stage of an adversary's attack.

5. The LRMF Should Require Agencies and Their Officials to Develop Shifting Defensive Environments

Building from the previous recommendation, constantly changing an environment may ensure an adversary who has gained access or deployed malicious code cannot maintain access to a system.[147] Moreover, the adversary

142. CLARKE & KNAKE, *supra* note 2, at 82–83.

143. Cloud computing can be defined as

> [A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [e.g., networks, servers, storage, applications, and services)] that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

See Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. STANDARDS & TECH. (Sept. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

144. *See supra* notes 134–137 and accompanying text.

145. CLARKE & KNAKE, *supra* note 2, at 52–66; Ali, *supra* note 4, at 41 n.222.

146. CLARKE & KNAKE, *supra* note 2, at 52–66; Ali, *supra* note 4, at 41 n.222.

147. CLARKE & KNAKE, *supra* note 2, at 52–66; Ali, *supra* note 4, at 42.

would be forced to think about the cost's association with an attack, and whether the time, effort, and expense associated with an operation offers only a marginal benefit or something more.[148] Essentially, you've found another way into their kill-chain, albeit by forces of economics through a sheer technical cybersecurity practice. This promotes transformability or a new reality given that a network has been compromised.

6. The LRMF Should Focus on Zero Trust Networks

A Zero Trust network uses an information technology model that requires a draconian process for identify verification.[149] It assumes a set of assumptions that every attempt to access the network is hostile.[150] Verification is required whether a user is internal or external to a network.[151] Locality is not sufficient for access; every device, user, or traffic request must be authenticated; written policies pull from a variety of sources via one authoritative cybersecurity theory.[152]

Technical practices include micro segmentation, the ability to break apart security perimeters into smaller and manageable zones, and separation access to parts of the network.[153] These practices assist in creating a layered defense and promoting the "kill chain" discussed above.[154] It may also require multi-factor identification, for example, not only allowing access by use of password but also requiring Public-Key authentication.[155] Lastly, it may include restricted access and limited permissive access for certain devices that connect to a network.[156]

Keeping the focus on Zero Trust networks assists in resiliency, as it serves as an initial defense to malicious actors' access to a network.[157] If mandated by law, cybersecurity may become much more achievable for NSSs.

---

148. CLARKE & KNAKE, *supra* note 2, at 52–66; Ali, *supra* note 4, at 34–37.

149. *See Zero Trust Security, What's a Zero Trust Network?*, CLOUDFLARE https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/ (last visited Apr. 7, 2021); *see also* Evan Gilman & Doug Barth, *Chapter 1 Zero Trust Fundamentals*, O'REILLY (2017), https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html (last visited Apr. 7, 2021).

150. *Zero Trust Security*, *supra* note 149; Gilman & Barth, *supra* note 149.

151. *Zero Trust Security*, *supra* note 149; Gilman & Barth, *supra* note 149.

152. *Zero Trust Security*, *supra* note 149; Gilman & Barth, *supra* note 149.

153. *Zero Trust Security*, *supra* note 149; Gilman & Barth, *supra* note 149.

154. *See supra* Part V.A.4.

155. National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 220, 133 Stat. 1198 (Dec. 20, 2019).

156. *Id.*

157. *Id.*

7. The LRMF Should Look to the Horizon for SASE Systems

SASE stands for Secure Access Service Edge.[158] First described by the research company Gartner, SASE stands for the proposition that cybersecurity can be offered as a convergence of WAN and network security services.[159] SASE delivers security as a service into a single model for cloud-based systems.[160] Services are based upon the identity, enterprise, security policies, context, and a continuous assessment of risk and trust.[161] This allows a level of flexibility and cost savings as cybersecurity would be encapsulated in one service through the implementation of many cybersecurity tools.[162]

Given the U.S. government's approach and enthusiasm for cloud computing models, this may be an important addition to the LRMF. Resiliency could be achieved because it would become a more manageable information technology portfolio, satisfying all cybersecurity products into a product that offers the dynamics of multiple systems that are difficult to track. Given its inherent dynamics, it would be less likely to be a single point of failure.

B. Other Areas of Law Can Lend Themselves to Assist the LRMF in Promoting Resiliency

It may be the case that existing areas of law outside of traditional cybersecurity regimes should be included in the LRMF. There are many, but two authorities are standouts regarding the needs of rapid technology development to protect NSSs from emerging threats such as quantum supremacy.[163]

1. Cooperative Research and Development Agreements

Cooperative Research and Development Agreements provided in 15 U.S.C. § 3710a and 10 U.S.C. § 2371a allows federal agencies to enter into agreements with non-federal parties to develop technology, if the government maintains license to practice the intellectual property (IP) developed.[164] This is helpful because it overcomes barriers found in the normal procure-

158. Matt Conran, *SASE: Redefining the Network and Security Architecture* (Nov. 25, 2019 10:54 AM PST), NETWORK WORLD (Nov. 25, 2019, 10:54 AM), https://www.networkworld.com/article/3481519/sase-redefining-the-network-and-security-architecture.html; *see also What is SASE?*, PALO ALTO NETWORKS, CYBERPEDIA, https://www.paloaltonetworks.com/cyberpedia/what-is-sase (last visited Apr. 7, 2021).

159. Conran, *supra* note 158; *What is SASE?*, *supra* note 158.

160. Conran, *supra* note 158; *What is SASE?*, *supra* note 158.

161. Conran, *supra* note 158; *What is SASE?*, *supra* note 158.

162. Conran, *supra* note 158; *What is SASE?*, *supra* note 158.

163. 10 U.S.C. § 2371a (1997); 15 U.S.C. § 3710a (2000); 10 U.S.C. § 2371 (2017); 10 U.S.C. § 2371b (2019).

164. 10 U.S.C. § 2371a; 15 U.S.C. § 3710a.

ment process, allowing high returns on investment, and more readily available operational technologies.[165] Moreover, it overcomes the issue of the federal government's inability to own copyrights—except by transfer—by allowing ownership of such right to the cooperative party, if such program is considered under the ambit of copyright law.[166] Defensive technologies may be deployed without risk of public disclosure for malicious parties to take advantage of initially.[167] This occurs because, although the government maintains a license to practice the IP, it may not disclose the IP due to the non-federal party's ownership status. Such rapid development and deployment of technologies may assist national security systems in obtaining defensive technologies needed to withstand malicious actors' attacks, thus remaining operable.

2. For Department of Defense Organizations, the Use of Other Transaction Authority May Assist the LRMF in Developing Resiliency

Through the use of Other Transaction Authority,[168] found in 10 U.S.C. § 2371 and 10 U.S.C. § 2371b, Department of Defense organizations are

165. *Cooperative Research and Development Agreement (CRADA) Program Overview*, DEF. INFO. SYS. AGENCY, https://www.disa.mil/About/CTO/CRADA-Process-Overview (last visited Apr. 7, 2021).

166. 17 U.S.C. § 105(a) (2019). It is debatable whether aspects of computer programming are more suited under patent law. *See* David S. Levitt, *Copyright Protection for United States Government Computer Programs*, 40 IDEA 225, 227–28 (2000).

167. Indeed, as Lucas Kello argues in an essay published in *Bytes, Bombs, and Spies*, the existence of a "sovereignty gap"—private sector's lack of confidence in government to protect them from malicious actors, where government has maintained the resources and legal authority alone to conduct cyber operations—is caused by new entrants into the operational cyber domain. *See* Lucas Kello, *15 Privante Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap?*, *in* BYTES, BOMBS, AND SPIES 357–74 (Herbert Lin & Amy Zegart eds., 2018). These new entrants include hacktivist, state controlled third parties, and sophisticated cyber gangs. *Id.* He notes that the boundary between economic and national security domains has merged. *Id.* at 358. This has caused the private sector to develop emerging technologies for its own active defense measures employed carefully to ensure they do not breach criminal law. *Id.* at 358–59. Because the private sector, not subject to draconian procurement processes of the federal government, can develop and employ emerging technologies for defensive purposes at exceeding rates, the federal government should take advantage of this through information sharing and partnership. *Id.* at 367. As related to this Article, this will promote "strategic depth" and "tactical flexibility" as defensive cybersecurity measures may outpace offensive actions by malicious actors. *Id.* at 362, 366–67.

168. MOSHE SCHWARTZ & HEIDI M. PETERS, CONG. RSCH. SERV., R45521, DEPARTMENT OF DEFENSE USE OF OTHER TRANSACTION AUTHORITY: BACKGROUND,

granted the authority to use agreements (not contracts) to develop joint ventures; partnerships; consortia; or agency partnerships for advanced research projects.[169] This also includes certain prototype projects.[170] Both authorities are subject to limitations, but the important point is that, as with the proceeding recommendation, it allows an exemption from the traditional procurement process.[171] Moreover, certain benefits include attracting non-traditional contractors, which may be congruent with bridging the cultural and generational differences between the new tech community and the traditional defense industry.[172] Lastly, it offers a defined mechanism to pool resources that may not be available through federal appropriation means.[173] This type of legal mechanism may assist the LRMF in deploying technologies needed for national security system resiliency through the use of an existing legal regime.

VI. CONCLUSION

Broad concepts are ideal in building new frameworks or thinking about change to any subject matter. The importance of resiliency is key to true risk management because it offers an idealistic concept that may change the way agencies think of cybersecurity for NSSs akin to paradigm shifting. With emerging threats such as quantum supremacy, the concept of resiliency becomes all the more important. The LRMF mandates that agencies and officials take their responsibility seriously to conduct the mental exercise of insuring mitigation of risk to NSSs, as opposed to existing normative regimes.[174] Merely managing risk may not be enough, especially if it is narrowly focused on technical aspects of mitigation. Instead, by requiring the ability to not only withstand the impacts of risk but also to recover and adapt to ensure operability as a legal duty, the LRMF may provide a solution for this ever-emerging threat and many others. The recommendations put forth in this Article assist in such an endeavor.

ANALYSIS, AND ISSUES FOR CONGRESS (2019), https://fas.org/sgp/crs/natsec/R45521.pdf.

169. 10 U.S.C. § 2371 (2017); 10 U.S.C. § 2371b (2019).

170. 10 U.S.C. § 2371b(a)(1).

171. *See* 10 U.S.C. § 2371; 10 U.S.C. § 2371b; 10 U.S.C. § 2371b(a)(1); *see also* 10 U.S.C. § 2371a (1997); 15 U.S.C. § 3710a (2000).

172. 10 U.S.C. § 2371; 10 U.S.C. § 2371b.

173. 10 U.S.C. § 2371; 10 U.S.C. § 2371b.

174. *See supra* Part III.