Virtual Checkpoints and Cyber-*Terry* Stops: Digital Scans To Protect the Nation's Critical Infrastructure and Key Resources

Scott J. Glick*

INTRODUCTION

In the twenty-first century, the Internet has revolutionized our ability to communicate, socialize and engage in commerce, and has become an "essential part of daily life of millions of Americans."[1] While it may have begun as a Department of Defense project to create a computer network that could survive a nuclear war, and in its earliest phases was used as a means of communication between academics, scientific researchers, and the government,[2] today the Internet "is a global network of interconnected communication and information systems."[3] That is both good news and bad news because the same Internet that connects us to each other and to the world also connects the world to the "nervous system of the country,"[4] including our nation's critical infrastructure and key resources.[5] Moreover,

* Senior Counsel, National Security Division, U.S. Department of Justice. This article has been reviewed for publication by the Justice Department in accordance with 28 C.F.R. §17.18. The views expressed in this article are solely those of the author and do not necessarily reflect the views of the Justice Department. The author wishes to thank Stephen Dycus, Stephen Vladeck, David Rosenberg, Mark Eckenwiler, Jordan Strauss, Joshua Geltzer, and Dena Roth for their review and comments on an earlier draft of this article.

1. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1005 (2010).

2. *See* Barry M. Leiner et al., A Brief History of the Internet, INTERNET SOCIETY, http://www.isoc.org/internet/history/brief.shtml/.

3. Todd M. Hinnen, *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COLUM. SCI. & TECH. L. REV. 5, 8 (2004).

4. *Cybersecurity: Evaluating the Administration's Proposals: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary,* 112th Cong. 4 (2011) (statement of Associate Dep. Att'y Gen. James A. Baker), *available at* http://www.fednews.com/printtranscript.htm?id=20110621t3839 [hereinafter Cybersecurity Hearing]; *see also* Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 168 (2008) ("[C]omputer networks are the 'nervous system' that ties together and controls . . . components of our national infrastructure.").

5. The definitions of "critical infrastructure" and "key resources" have been described as "evolutionary" and "ambiguous." John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification* (Cong. Res. Service RL 32631), Oct. 1, 2004, at 2. At the present time, the term "critical infrastructure" means "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national

while the Roman Empire may have been able to control the roads that it built to enable its empire to flourish,[6] neither federal nor state governments own all of the "virtual roads" that exist in cyberspace.[7] Indeed, the private sector, rather than the government, owns "most of our critical cyber infrastructure."[8]

To be sure, the federal government has taken steps to employ computer intrusion and detection technology to protect its own computer networks.[9] The government's ability to digitally scan private-to-private electronic or wire communications that are transiting the ".com" or ".org" domains for malicious digital codes,[10] however, raises a fundamentally different Fourth

economic security, national public health or safety, or any combination of those matters." Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, §1016(e), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified at 42 U.S.C. §5195c(e) (2006)). In addition, the term "key resources" means "publicly or privately controlled resources essential to the minimal operations of the economy and government." Homeland Security Act of 2002, §2(9), Pub. L. No. 107-296, 116 Stat. 2135 (2002) (codified at 6 U.S.C. §101(10) (2006)).

6. As Federal Bureau of Investigation Director Robert Mueller aptly noted during a cybersecurity speech he gave at Penn State University in 2007, while the Roman Empire was able to flourish for hundreds of years, in the end it was overrun by millions of invaders who used the same roads that had originally been built to spread Roman civilization and influence. *See* Steven R. Chabinsky, *Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line*, 4 J. NAT'L SECURITY L. & POL'Y 27, 29 (2010).

7. Arguably, the roads in cyberspace are more physical than virtual because the basic architecture of the network – including the computers, wires, cables, servers, routers and switches that allow it to function – physically exist at various locations around the country. *See* Cybersecurity Hearing, *supra* note 4 (testimony of Associate Dep. Att'y General James A. Baker) (the "Internet is a physical thing, and it exists in different places" in the physical world); *see also* BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 84 (2010) (the Internet "connects different physical networks").

8. William C. Banks & Elizabeth Rindskopf Parker, Introduction, *Cybersecurity Symposium: National Leadership, Individual Responsibility*, 4 J. NAT'L SECURITY L. & POL'Y 7, 9 (2010); *see also* THE NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 398 (2004) ("[T]he private sector controls 85 percent of the critical infrastructure in the nation.").

9. The Department of Homeland Security has begun to use "Einstein 2" as a computer network intrusion detection system to "observe in near-real time the packet header and packet content of all incoming and outgoing Internet traffic of Federal Systems ('Federal Systems Internet Traffic') for the 'signatures' of malicious computer code used to gain access to or to exploit Federal Systems." *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch*, Memorandum Opinion for the Counsel to the President, Office of Legal Counsel (Jan. 9, 2009), at 3, *available at* http://www.justice.gov/olc/2009/e2-issues.pdf [hereinafter OLC Legal Issues Memorandum]; *see also* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

10. As used in this article, the term "malicious digital codes" refers to any kind of computer virus, worm, bot-net, spyware, malware, Trojan horse, network exploitation or infiltration code, or any other malicious digital or computer codes that enable malicious actors to inflict harm or obtain control of the computers, networks and devices that control and operate the nation's critical infrastructure and key resources. *See* OLC Legal Issues

Amendment[11] issue than the government's ability to digitally scan incoming and outgoing communications on the ".gov" or ".mil" domains. If one were to use a criminal investigatory lens, one would conclude that the "Fourth Amendment ordinarily requires a warrant for the collection of the contents of Internet communications."[12] Under this view, a Title III[13] wiretap order to obtain the contents of those communications in real time must be issued by a "neutral and detached authority" and the order must be based on individualized suspicion.[14] A "foreign intelligence" lens would also generally require a court order.[15]

But what if, instead of seeking evidence of criminal activity or foreign intelligence information, the government used a different lens and employed computer intrusion and detection technology at certain specific digital locations on the Internet primarily for protective purposes?[16] In the physical world, the government can engage in a variety of protective activities, and the Fourth Amendment does not always require the government to have individualized suspicion or obtain a court order. For example, government agents can conduct international border searches, establish sobriety checkpoints, and engage in security screening searches at domestic airports – all within a legal framework that does not require individualized suspicion of criminal activity or a court order.[17] The question then is whether, in the absence of individualized suspicion and a court order, technology that digitally scans Internet communications for malicious digital codes without initially exposing the contents of those communications to human review[18] may be used without running afoul of

Memorandum, *supra* note 9 at 3 n.3; NAT'L INSTITUTE OF JUSTICE, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER NETWORKS 55 (2007), *available at* http://www.ncjrs.gov/ pdffiles1/nij/210798.pdf.

11. The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

12. Kerr, *supra* note 1, at 1039.

13. *See* Title III, Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §802, 82 Stat. 197, 212-223 (codified as amended at 18 U.S.C. §§2510-2520 (2006)) [hereinafter Title III].

14. See Berger v. New York, 388 U.S. 41, 54 (1967), and its progeny.

15. *See generally* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§1801-1811(2006)).

16. For a discussion of some of the government's military authorities in cyberspace, which are beyond the scope of this article, see Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63 (2010); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87 (2010).

17. *See infra* Section II.

18. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 535 (2005) (a search is best described as the process by which "data is exposed to

the Fourth Amendment. Moreover, if there is a reasonable basis to believe that a malicious digital code may be present, an equally important question is what mechanisms can be put in place to ensure that remedial and other actions taken by the government to protect the nation's critical infrastructure and key resources are reasonable and constitutional.

As background for this article, Part I provides an overview of the cybersecurity risks, as identified by various experts, to the nation's critical infrastructure and key resources. Part II then examines the legal frameworks from the physical world that govern international border searches, sobriety and other checkpoints on public highways, searches by narcotics-detection dogs, screening searches at airport security checkpoints, and *Terry*-stops, as well as the government's authority to quarantine and isolate persons who have communicable diseases. Part III then argues that by using the correct Fourth Amendment lens, these fairly well established legal frameworks from the physical world strongly support the existence of a new cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements. If appropriate legislation is enacted, the cybersecurity exception will enable the government to conduct reasonable and limited digital scans at virtual checkpoints in cyberspace, when the programmatic purpose of those scans is to identify malicious digital codes that may be attacking the nation's critical infrastructure and key resources. Part III therefore proposes that the Congress consider and enact sensible new legislation that will permit the government to conduct these digital scans and take remedial and other actions to protect the nation without running afoul of the Fourth Amendment and existing law.

I. CYBERSECURITY RISKS TO THE NATION'S CRITICAL INFRASTRUCTURE AND KEY RESOURCES

In his May 2009 Cyberspace Policy Review, President Barack Obama declared that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century."[19] Two years later, President Obama unveiled a comprehensive cybersecurity legislative proposal to protect the "Nation's critical infrastructure, and the Federal government's own networks and computers."[20]

human observation").

19. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE iii (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; s*ee also* Walter Gary Sharp, Sr., *The Past, Present, and Future of Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 13, 13 ("The cyber threat is the most pervasive and pernicious threat facing the United States today."). *See generally* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

20. *See* Press Release, White House Office of the Press Secretary, Fact Sheet:

The rationale for comprehensive cybersecurity legislation is clear. The cybersecurity risks[21] facing the nation's critical infrastructure and key resources have dramatically increased over the last decade[22] and are frequently described in ominous tones. For example, during his recent confirmation hearing for Secretary of Defense, then Central Intelligence Agency Director Leon Panetta stated that the "next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, and our governmental systems."[23] Senator Susan M. Collins, Ranking Member of the U.S. Senate's Homeland Security and Governmental Affairs Committee and a cosponsor of the "Cybersecurity Act of 2012,"[24] has stated that the nation faces the threat of a "cyber 9/11."[25] In addition, Senator Jay Rockefeller, Chairman of the U.S. Senate's Committee on Commerce, Science and Technology and cosponsor of the "Cybersecurity Act of 2012,"[26] has also stated that a "major cyber attack could shut down our Nation's most critical

Cybersecurity Legislative Proposal, *available at* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

21. While "risk" and "threat" are often used interchangeably, experts have cautioned against exclusively looking at threats to assess cybersecurity risks. Instead, they recommend use of the "classic risk formula." *See* Chabinsky, *supra* note 6, at 35 ("Risk = Threat x Vulnerability x Consequence.").

22. Cybersecurity Hearing, *supra* note 4, at 2 (statement of Associate Dep. Att'y Gen. James A. Baker), *available at* http://www.judiciary.senate.gov/pdf/11-06-21%20Joint%20of%20Statement%20of%20James%20Baker,%20Greg%20Schaffer,%20and%20Ari%20Schwartz.pdf. *See* OLC Legal Issues Memorandum, *supra* note 9, at 2 ("Over the past several years, Federal Systems have been subject to sophisticated and well-coordinated computer network intrusions and exploitations on an unprecedented scale. The Intelligence Community has determined that those malicious network activities pose a grave threat to national security."); *see also* John Rollins & Anna Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Cong. Res. Service R40427) Mar. 10, 2009, at 2 ("Threats to the U.S. cyber and telecommunications infrastructure are constantly increasing and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests." (footnotes omitted)).

23. *See Nomination of Leon Panetta for Secretary of Defense: Hearing Before the S. Comm. on Armed Services*, 112th Cong. 25 (2011) (testimony of CIA Director Leon Panetta), *available at* http://armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf. Most recently, FBI Director Robert Mueller testified that "the cyber threat will equal or surpass the threat from counterterrorism in the foreseeable future." *Worldwide Threat Assessment of the U.S. Intelligence Committee: Hearing Before the H. Permanent Select Comm. on Intelligence*, 112th Cong., 2d Sess. (2012) (testimony of FBI Director Robert Mueller).

24. S. 2105, 112th Cong. (2012).

25. *See* Press Release, Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses (June 10, 2010), *available at* http://www.lieberman.senate.gov/index.cfm/news-events/news/2010/6/lieberman-collins-carper-unveil-major-cybersecurity-bill-to-modernize-strengthen-and-coordinate-cyber-defenses.

26. S. 2105, 112th Cong. (2012).

infrastructure: our power grid, telecommunications, [and] financial services . . . ."[27]

Similarly, former government officials have spoken about the serious cybersecurity risks facing the nation's critical infrastructure and key resources. For example, Michael Chertoff, former Secretary of Homeland Security, has stated that "[n]etwork electronic warfare can cripple or paralyze domestic and civilian systems."[28] Richard Clarke, former Cybersecurity Advisor to President Obama, has also warned that foreign intelligence services have penetrated the control systems of the U.S. electric power grid and have left behind "logic bombs" and "trap doors."[29]

The primary reason for these concerns is clear. As former Director of National Intelligence Dennis Blair has stated, the "connectivity between information systems, the Internet and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures."[30] As a result, we live in a world where a potential cyber attack is not just a criminal issue affecting individuals or businesses, but one which represents a broader economic risk to the nation.[31] Today, the

27. *Cybersecurity: Next Steps to Protect Our Critical Infrastructure*: *Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. 2 (2009) (statement of Sen. Jay Rockefeller), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg57888/pdf/CHRG-111shrg57888.pdf; *see also* JACK GOLDSMITH, BROOKINGS INSTITUTION, THE CYBERTHREAT, GOVERNMENT NETWORK OPERATIONS, AND THE FOURTH AMENDMENT 1 (2010), *available at* http://www.brookings.edu/papers/2010/1208_4th_amendment_goldsmith.aspx ("[T]he national communications network is swarming with known malicious cyber agents that raise the likelihood of an attack on a critical infrastructure system that could cripple our economic or military security.").

28. Michael Chertoff, Foreword, *Cybersecurity Symposium: National Leadership, Individual Responsibility*, 4 J. NAT'L SECURITY L. & POL'Y 1, 1 (2010); *see also Cyber Security: Responding to the Threat of Cyber Crime and Terrorism*: *Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 112th Cong. 5 (statement of Stewart Baker, former Ass't Sec'y for Policy, Dep't of Homeland Security), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16a9959&wit_id=e655f9e2809e5476862f735da16a9959-2-2 (warning that the tools the "stuxnet" virus deployed could "just as easily be used to bring down the power grid for a city or a region").

29. Richard A. Clarke, *Obama's Challenge in Cyberspace*, HUFF. POST, (May 8, 2009, 10:29 AM), http://www.huffingtonpost.com/richard-a-clarke/obamas-challenge-in-cyber_b_199926.html; *see also* RICHARD CLARKE AND ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2010).

30. *Annual Threat Assessment of the Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. 38 (2009) (testimony of Director of National Intelligence Dennis Blair), *available at* http://www.dni.gov/testimonies/20090212_testimony.pdf; *see also* Ellen Nakashima, *U.S. Systems are Vulnerable to Hackers*, WASH. POST, Oct. 2, 2011, at A3 (explaining that the threat exists "because machines running the nation's plants and other crucial systems are increasingly interconnected").

31. *Annual Threat Assessment of the Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. 38 (2009) (testimony of Director of National Intelligence Dennis Blair), *available at* http://www.dni.gov/testimonies/20090212

"full dimension" of the cybersecurity risks to the nation include "substantial risks to the *command and control* of important physical assets such as electric power grids, water supply, and other critical infrastructure."[32]

Connectivity, however, is not the only cybersecurity challenge facing the nation. Developing and implementing strategic or tactical plans to protect the nation's critical infrastructure and key resources is complex because experts have identified numerous "threat vectors," including "supply chain and vendor access, remote access, proximity access, and insider access."[33] The supply chain and vendor access threat results from the fact that the "global economy" enables our nation to "compete and purchase services in an expanded market" which has "substantially increased our vulnerability to adversarial manipulation of our software and hardware."[34] By way of contrast, the remote access threat comes from "computer network intrusions or 'hacking.'"[35] On the other hand, the proximity access threat refers to the "abilities our adversaries have when they are physically close to our networks but not directly inside them," and the insider threat comes from trusted persons who are given access to computer networks and systems, such as "employees, contractors, and trusted business partners."[36]

The concern about insiders, however, does not arise only from malicious actors. There is no security patch for cyber-stupidity, and an employee who inserts a virus-laden USB thumb drive into a networked computer may be as much a threat as the employee who intends to do

_testimony.pdf (arguing that a successful cyber attack could "severely impact the national economy"); *see also* Burstein, *supra* note 4, at 168 ("[M]odern attacks threaten to target infrastructure that is integral to the economy, national defense, and daily life.").

32. Chabinsky, *supra* note 6, at 28 n. 3 (emphasis supplied); *see also* DEP'T OF HOMELAND SEC., PRIMER CONTROL SYSTEMS CYBER SECURITY FRAMEWORK AND TECHNICAL METRICS (2009), *available at* http://www.us-cert.gov/control_systems/pdf/Metrics_primer_v9_7-13-09_FINAL.pdf ("Electronic control systems that operate much of the Nation's critical infrastructure are increasingly connected to public networks, including the Internet . . . and are at greater risk than before from externally initiated cyber attacks."); Goldsmith, *supra* note 27, at 1 ("[O]ur energy supply, our means of transportation, and our military defenses are dependent on vast, interconnected computer and telecommunications networks . . . ."); Dominic Basulto, *Digital Deterrents: Preventing a Pearl Harbor of Cyberspace*, WASH. POST (Oct. 17, 2011), http://www.washingtonpost.com/blogs/innovations/post/digital-deterrents-preventing-a-pearl-harbor-of-cyberspace/2010/12/20/gIQASNKyoL_blog.html ("The Internet has become the back door and front door to controlling nearly every aspect of our national infrastructure.).

33. Chabinsky, *supra* note 6, at 32.

34. *Id*.; *see also* Josh Smith, *Homeland Security Official: Some Foreign-Made Electronics Compromise Cybersecurity*, NATIONAL JOURNAL (JULY 7, 2011, 3:23 PM), http://www.nationaljournal.com/tech/homeland-security-official-some-foreign-made-electronics-compromise-cybersecurity-20110707.

35. Chabinsky, *supra* note 6, at 34.

36. *Id*.; *see also* Susan Candiotti, *Homeland Security Warns of Potential Threats to Utilities*, CNN (July 21, 2011), http://www.cnn.com/2011/US/07/21/terror.warning.utilities/.

harm.[37] Finally, and perhaps the biggest cybersecurity challenge, intrusion detection systems also face what some experts call the "zero day" threat because "malicious actors develop new malware continually," and anti-virus and other intrusion programs "cannot detect and stop malware that no one has seen before."[38]

Under the single-party consent exception to Title III,[39] the government is able to use intrusion and detection technology to protect the ".gov" and ".mil" domains.[40] The primary legal issue therefore relates to the ".com" and other private sector domains. While existing statutes enable employees of communications service providers to monitor their own networks to protect their "property" rights, to perform "mechanical or service quality control checks," and to intercept and disclose the content of electronic communications if it is "necessarily incident to the rendition" of those services,[41] the prevailing conventional legal theory is that if the government were to use an intrusion and detection system to monitor "private-to-private communications, it would likely be considered an interception under the electronic surveillance laws, which require a court order."[42] As a result, while increased public awareness[43] of cyber threats and better policy

37. *See* Frank L. Greitzer et al., *Combating the Insider Cyber Threat*, IEEE SECURITY & PRIVACY, Jan.-Feb. 2008, at 61, 61, *available at* www.cert.org/archive/pdf/combatthreat0408.pdf ("The insider threat is manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies.").

38. Cybersecurity Hearing, *supra* note 4, at 4; *see also* Lin, *supra* note 16, at 65 n.7 ("The term [zero day attack] refers to the fact that the vulnerability has been known to the defender for zero days.").

39. *See* 18 U.S.C. §2511(2)(c) (2006) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire . . . or electronic communication, where . . . one of the parties to the communication has given prior consent to such interception.").

40. The Office of Legal Counsel of the U.S. Department of Justice has opined that when "log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system," the Einstein 2 intrusion and detection technology employed by Executive Branch departments and agencies is lawful. *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, Memorandum Opinion for an Associate Deputy Attorney General, Office of Legal Counsel 1 (Aug. 14, 2009), *available at* http://www.justice.gov/olc/2009/legality-of-e2.pdf; *see also* OLC Legal Issues Memorandum, *supra* note 9.

41. *Compare* 18 U.S.C. §2511(2)(a)(i) (2010), *with* 18 U.S.C. §2702(b)(5) (2010).

42. Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119, 124 (2010). By way of contrast, "metadata" information, which includes the "addressing information for e-mails, IP addresses of visited Web sites, routing information that tracks a communication's path on the Internet, and possible traffic volume information . . . does not implicate the Fourth Amendment." Goldsmith, *supra* note 27, at 11.

43. *See* 156 Cong. Rec. S7944-S7946 (daily ed. Nov. 17, 2010) (statement of Sen. Whitehouse) ("One of the principal findings of our cyber task force was that most cyber threats – literally the vast majority of cyber threats – can be countered readily if Americans simply allowed automatic updates to their computer software, ran up-to-date antivirus

choices, including "multiple solutions" to "the attribution problem"[44] will improve the nation's cybersecurity, and while enhanced partnerships between the government and the private sector, as well as economic incentives, will also lead to "best" (as well as "next") cybersecurity practices,[45] reexamining conventional legal theories is essential when "[c]omputer systems integral to the infrastructure, economy, and defense of the United States are under constant attack by a growing array of adversaries."[46] Stated another way, and to paraphrase former Attorney General John Ashcroft, the cybersecurity risks facing the nation require us to think "outside the box" but "inside the Constitution."[47]

II. LEGAL FRAMEWORKS FROM THE PHYSICAL WORLD

The Fourth Amendment protects against "unreasonable searches and seizures." A "search" within the meaning of the Fourth Amendment takes place whenever the government intrudes upon "an expectation of privacy that society is prepared to consider reasonable."[48] This formulation, which flows from the formulation by Justice Harlan in his concurring opinion in

programs, and exercised reasonable vigilance when surfing the Web and opening e-mails.").

44. *See* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 571, 598 (2011). Former and current government officials, as well as some lawmakers, have stated that the United States should create a new ".secure" Internet to eliminate the threats that anonymity poses to the current Internet. Under this proposal, users would need certified credentials to access the new ".secure" Internet for critical infrastructure. *See* Aliya Sternstein, *Former CIA Director: Build A New Internet To Improve Cybersecurity*, NATIONAL JOURNAL (July 7, 2011), http://www.nationaljournal.com/nationalsecurity/former-cia-director-build-a-new-internet-to-improve-cybersecurity-20110707.

45. *See* William Jackson, *Group Proposes Economic Incentives To Improve Cybersecurity*, GOVERNMENT COMPUTER NEWS (Dec. 3, 2009), http://gcn.com/Articles/2009/12/03/ISA-security-framework-120309.aspx.

46. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT (2011), *available at* http://www.justice.gov/oig/reports/FBI/a1122r.pdf. *See also* Nakashima, *supra* note 30, at A3 ("[M]alicious computer code [can] cripple critical systems that millions of people rely on for food, fuel, safe water and more."); Ed O'Keefe, *Janet Napolitano: Hackers Have "Come Close" to Major Cyber Attack*, WASH. POST. (October 27, 2011), http://www.washingtonpost.com/blogs/federal-eye/post/janet-napolitano-hackers-have-come-close-to-major-cyber-attack/2011/10/27/gIQAZgQgMM_blog.html.

47. *See Ashcroft Evaluates the War on Terror*, CBS NEWS (Feb. 13, 2003), http://www.cbsnews.com/stories/2003/02/13/terror/main540422.shtml. *See also* Mark D. Young, *Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 STAN. L. & POL'Y REV. 11, 21 (2011) ("The government is attempting to protect national interests from myriad cyberspace threats and shift its organizational structures to better manage its limited cyberspace resources. It is doing this, however, without adjusting one of the biggest cyber vulnerabilities facing the country: insufficient legal authorities to allow federal action in the cyber domain.").

48. United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed.").

Katz v. United States,[49] breaks down into a "two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"[50] Thus, if the government's conduct violates a person's reasonable expectation of privacy, or if the government's conduct involves a trespass or a physical intrusion upon a constitutionally protected "effect" or area, then the courts will consider the government's conduct to be a "search" within the meaning of the Fourth Amendment.[51] By way of comparison, "seizures" within the meaning of the Fourth Amendment only take place when there has been a "meaningful interference with an individual's possessory interests in the property,"[52] or when there has been a "governmental termination of freedom of movement *through means intentionally applied*."[53] As a result, when the government's actions constitute a search or a seizure within the meaning of the Fourth Amendment, they must not be "unreasonable."[54]

A Fourth Amendment search or seizure that is conducted without judicial authorization is "per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions."[55] These exceptions include, but are not limited to, consent searches,[56] searches of vehicles,[57] searches incident to arrest,[58] and searches

49. 389 U.S. 347, 360-361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"). *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §2.1(b)-(d) (4th ed. 2004).

50. California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

51. *See* United States v. Jones, 132 S. Ct. 945, 953 (2012) (holding that placing a GPS tracking device on a vehicle for the purpose of obtaining information is a "search" but that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to Katz analysis") (emphasis in original); *see also* Illinois v. Andreas, 463 U.S. 765, 771 (1983).

52. *Jacobsen*, 466 U.S. at 113.

53. Brower v. County of Inyo, 489 U.S. 593, 597 (1989) (emphasis in original).

54. *See* Illinois v. McArthur, 531 U.S. 326, 330 (2001) (holding that the "'central requirement'" of the Fourth Amendment is "reasonableness").

55. Katz v. United States, 389 U.S. 347, 357 (1967) (footnotes omitted).

56. *E.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (holding that consent is one of the "specifically established exceptions to the requirements of both a warrant and probable cause").

57. *E.g.*, Carroll v. United States. 267 U.S. 132 (1925) (holding that because they are highly mobile, a warrant is not required to search a vehicle if police have probable cause to believe the vehicle contains evidence of a crime).

58. *E.g.*, Chimel v. California, 395 U.S. 752 (1969) (holding that when a person is lawfully arrested, the police may search the person and any area surrounding the person that is within his or her reach).

conducted when exigent circumstances exist.[59] Nonetheless, even under these exceptions, government searches and seizures are "ordinarily unreasonable in the absence of individualized suspicion of wrongdoing."[60]

Notwithstanding these cardinal principles and rules,[61] there are "limited circumstances" where the lack of individualized suspicion does not prevent the government from conducting a search without a judicial warrant. Indeed, for nearly a half a century, the Supreme Court has carved out "special needs"[62] and "administrative search"[63] exceptions to the Fourth Amendment; that is, circumstances where the government is able to intrude upon areas which are protected by the Fourth Amendment without regard to whether individualized suspicion exists.[64] As detailed below, in the special needs and administrative search cases, courts will examine whether the search furthers a "special need[], beyond the normal need for law enforcement."[65] These cases also look at the "programmatic purposes"[66] that are motivating the government's conduct to ensure that the government is seeking to protect against a "concrete danger."[67] Here, the programmatic

59. *E.g.*, Georgia v. Randolph, 547 U.S. 103, 117 n. 6 (2006) (holding that no warrant is required when evidence can be easily moved or destroyed, there is a threat to the public or the police, or the police are in "hot pursuit" of a suspect).

60. City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) (citing Chandler v. Miller, 520 U.S. 305, 308 (1997).

61. *Compare* Mincey v. Arizona, 437 U.S. 385, 390 (1978) (noting that the warrant requirement is a "cardinal principle"), *with Edmond*, 531 U.S. at 37 ("[W]hile such suspicion is not an 'irreducible' component of reasonableness . . . we have recognized only limited circumstances in which the usual rule does not apply.") (citation omitted).

62. *See*, *e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (random drug testing of student-athletes); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989) (drug tests for United States Customs Service employees seeking transfer or promotion to certain positions); Skinner v. Ry. Labor Executives' Assn., 489 U.S. 602 (1989) (drug and alcohol tests for railway employees involved in train accidents or found to be in violation of particular safety regulations).

63. *See*, *e.g.*, New York v. Burger, 482 U.S. 691, 702-704 (1987) (warrantless administrative inspection of premises of "closely regulated" business); Michigan v. Tyler, 436 U.S. 499, 507-509, 511-512 (1978) (administrative inspection of fire-damaged premises to determine cause of blaze); Camara v. Mun. Court of City & County of San Francisco, 387 U.S. 523, 534-539 (1967) (administrative inspection to ensure compliance with city housing code).

64. *See generally* 5 Wayne R. La Fave, *supra* note 49, at §10.1.

65. Chandler v. Miller, 520 U.S. 305, 313-314 (1997).

66. *See Edmond,* 531 U.S. at 45 ("[P]rogrammatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion.").

67. *Chandler*, 520 U.S. at 318-19. The special needs cases also provide a key doctrinal basis for a foreign intelligence exception to the Fourth Amendment's warrant requirement based on the "programmatic purpose" of the surveillance, and a "legitimate objective beyond ordinary crime control." *See In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011-1012 (FISA Ct. Rev. 2008); *In re* Sealed Case, 310 F.3d 717, 741-42 (FISA Ct. Rev. 2002).

purpose behind a digital scan at a virtual checkpoint would be to minimize the risk of catastrophic damage to the nation's critical infrastructure and key resources from a cyberattack, clearly a compelling and "legitimate objective" of the "highest magnitude" that goes "well beyond" ordinary crime control.[68]

While a compelling governmental need is a necessary prerequisite, alone it is not a sufficient basis to uphold the constitutionality of a special needs or administrative search. The federal courts also consider other factors, and evaluate the reasonableness of the search by weighing the level of the intrusion and the privacy interests at stake.[69] As a result, this Part of the article will examine the special needs and administrative search cases, as well as other legal frameworks from the physical world, to determine whether, taken together, they support the existence of a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements.[70]

A. International Border Searches

In view of the "global" connectivity of the Internet,[71] it is appropriate to examine the legal framework that governs searches and seizures at the nation's international border. The earliest case in which the Supreme Court commented on international border searches was *Boyd v. United States*.[72] There, the Court noted that searches at the international border were first authorized by the same Congress that authorized the Bill of Rights and that the "members of that body did not regard searches and seizures of this kind as 'unreasonable,' and [did not consider them to be] embraced within the

68. *In re* Directives, 551 F.3d at 1011-1012 (finding a foreign intelligence exception to the fourth amendment because national security is of "the highest magnitude" and the "programmatic purpose [of the surveillance] involves some legitimate objective beyond ordinary crime control"); Cassidy v. Chertoff, 471 F.3d 67, 82 (2d Cir. 2006) ("[P]reventing or deterring large-scale terrorist attacks presents problems that are distinct from standard law enforcement needs and indeed go well beyond them."); O'Connor v. Ortega, 480 U.S. 709, 720 (1987) (plurality opinion) ("[These cases represent] 'exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'" (citation omitted)); *cf. Edmond*, 531 U.S. at 43 ("We are particularly reluctant to recognize exceptions to the general rule of individualized suspicion where governmental authorities primarily pursue their general crime control ends.").

69. *E.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 830-38 (2002) (holding that the school's interest in preventing drug use outweighed limited intrusion and reduced privacy interests); *accord* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664-65 (1995).

70. Professor Jack Goldsmith of Harvard Law School finds legal support for a "comprehensive government-mandated, government-coordinated intrusion-prevention system throughout the U.S. network" based, in part, on the "special needs" cases. *See* Goldsmith, *supra* note 27, at 6, 11-13.

71. *See* Hinnen, *supra* note 3, at 5; *see also id.* at 5 n. 20 (explaining the differences between the "Internet" and the "World Wide Web").

72. 116 U.S. 616 (1886).

prohibition of the [Fourth] Amendment."[73] Nearly 40 years later, the Court further commented on such searches for protective purposes. In *Carroll v. United States*,[74] the Court stated that a traveler may be stopped when he crosses "an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings and effects which may be lawfully brought in."[75] Thereafter, in a series of cases, the Court repeatedly upheld international border searches as part of the government's "longstanding right . . . to protect itself by stopping and examining persons and property crossing into this country."[76] More recently, in *City of Indianapolis v. Edmond*,[77] although it invalidated a drug checkpoint, the Supreme Court emphasized that its holding did "nothing to alter the constitutional status of . . . border checkpoints," which are grounded in "considerations specifically related to the need to police the border."[78]

The international border search doctrine applies whenever a person or goods enter the United States, irrespective of whether it is on land from an adjacent country, at a place where a ship docks, or the location where a flight arriving from a foreign nation lands for the first time,[79] even if that location is in the interior of the country, because that arrival point constitutes the "functional equivalent" of the international border.[80] Moreover, the permissible scope of such a border search is quite extensive,[81] and the federal courts have upheld searches of baggage, goods,

73. *Id*. at 623.

74. 267 U.S. 132 (1925).

75. *Id*. at 154.

76. *E.g*., United States v. Ramsey, 431 U.S. 606, 616 (1977) ("That searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration."); Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) ("It is undoubtedly within the power of the Federal Government to exclude aliens from the country. . . . It is also without doubt that this power can be effectuated by routine inspections and searches of individuals or conveyances seeking to cross our borders.") (citations omitted).

77. 531 U.S. 32 (2000).

78. *Id.*; *see also* United States v. Flores-Montano, 541 U.S. 149, 152 (2004) ("The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border.").

79. *See* 5 LaFave, *supra* note 49, at §10.5(a) (collecting cases); *cf*. 8 U.S.C. §1357(c) (2006) (immigration officials); 14 U.S.C. §89(a) (2006) (Coast Guard); 19 U.S.C. §§482, 1496, 1581(a) (2006) (customs officials).

80. *Almeida-Sanchez*, 413 U.S. at 273 ("[A] search of the passengers and cargo arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search.").

81. *See* 5 LaFave, *supra* note 49, at §10.5(a) (collecting cases).

automobiles, persons, and personal items and papers, including computers and electronic media.[82]

The legal principles that flow from an analysis of the international border search cases are clear: searches at the international border or its functional equivalent may be conducted by the government without a warrant and without individualized suspicion.[83] Any "person or thing coming into the United States is subject to search by that fact alone, whether or not there is any suspicion of illegality directed toward the particular person or thing to be searched."[84] As a result, the sovereign's right to protect itself at the digital international border should be at least as coextensive as its right to protect itself in the physical world.[85] Although there may not be a specific geographic boundary to the digital international border, electronic (or wire) communications in cyberspace which originate outside the United States clearly cross the "functional equivalent" of the international border at specific "routers," "switches," or other locations in the United States.[86] While a regulatory scheme that classifies certain malicious digital codes as contraband may be needed, that does not undermine the constitutionality of the government's use of technology to scan for malicious digital codes at the digital international border. The cybersecurity risks to the nation's critical infrastructure and key resources from these codes are "particularly acute"[87] to justify such a protective action by the government. Moreover, if government agents can conduct further searches of a letter at the international border in the physical world when

82. United States v. Arnold, 523 F.3d 941, 948 (9th Cir. 2008); United States v. Linarez-Delgado, 259 Fed. Appx. 506, 508 (3d Cir. 2007); United States v. Ickes, 393 F.3d 501, 506-07 (4th Cir. 2005).

83. *See* United States v. Montoyo de Hernandez, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant.").

84. United States v. Odland, 502 F.2d 148, 151 (7th Cir. 1974) ("There is substantial authority in those Circuits stating the power to search at international borders in the same sweeping terms as the regulation. Any person or thing coming into the United States is subject to search by that fact alone, whether or not there be any suspicion of illegality directed to the particular person or thing to be searched.").

85. United States v. Ramsey, 431 U.S. 606, 615-616 (1977).

86. *See* DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE vii (2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf ("Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."). *See also* Clark and Landau, *supra* note 44, at 574 (explaining that data and electronic communications are transported "on" or "over" the Internet in "packets – small units of data prefixed with delivery instructions" through a "mesh of specialized computers called routers").

87. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 47-48 (2000) ("Our holding also does not affect the validity of border searches or searches at places like airports and government buildings, where the need for such measures to ensure public safety can be particularly acute.").

they have a reasonable basis to believe that contraband may be present,[88] they should be able to conduct further searches of electronic communications entering the United States at the digital international border when there is a reasonable basis to believe that a malicious digital code may be present.

B. Sobriety and Other Checkpoints

Conducting digital scans of electronic communications entering the United States from abroad, however, will not provide a doctrinal basis for protecting against malicious digital codes that originate, or appear to originate,[89] inside the United States. The legal framework that governs sobriety checkpoints[90] on the nation's public highways, however, does have application to a legal framework that can be constructed to govern domestic virtual checkpoints. For example, in *Michigan Department of State Police v. Sitz,*[91] the Michigan State Police had established sobriety checkpoints at a number of selected sites along state roads in accordance with specific procedures.[92] All vehicles passing through the checkpoints were stopped by the police, and if signs of intoxication were observed, the driver would be directed to a location out of the traffic flow where the police would conduct further sobriety tests.[93] The protective purpose behind the sobriety checkpoints was clear: they were designed primarily to ensure highway safety and eliminate an "immediate, vehicle-bound threat to life and limb."[94]

A protective purpose alone, however, was not the only factor that led the Court to conclude that the sobriety checkpoints were constitutional. Indeed, at least three factors were considered essential to the validity of the sobriety checkpoints in *Sitz*: (1) the State's "interest" in preventing drunken driving; (2) the extent to which the system could "reasonably be said to advance that interest"; and (3) the "degree of intrusion on individual motorists who [were] briefly stopped."[95] Since the level of intrusion was minimal[96] and the program was reasonably effective, as compared to

88. *Ramsey,* 431 U.S. at 616.

89. Cyber attackers often use more than one computer to hide the actual origin of the attack. *See* Clark and Landau, *supra* note 44, at 582 ("Many attacks and exploits are *multi-stage* in character: for example, A penetrates computer B to use as a platform for penetrating C, which is then used to attack D.") (emphasis in original).

90. *See generally* R. Marc Kantrowitz et al., Annotation, *Validity of Police Roadblocks or Checkpoints for Purpose of Discovery of Alcoholic Intoxication – Post Sitz Cases*, 74 A.L.R.5th 319 (2011) (collecting cases).

91. 496 U.S. 444 (1990).

92. *Id*. at 447.

93. *Id*.

94. *See* City of Indianapolis v. Edmond*,* 531 U.S. 32, 43 (2000).

95. *Sitz,* 496 U.S. at 455.

96. The delay to drivers during the sobriety checkpoints upheld by the Supreme Court

traditional law enforcement techniques,[97] given the "magnitude of the drunken driving problem"[98] and the state's interest in "eradicating"[99] that problem, the program was not unconstitutional.[100]

The Supreme Court has also upheld the use of fixed immigration checkpoints without individualized suspicion.[101] Immigration checkpoint stops are "reasonable" under the Fourth Amendment because the state's interest in detecting the presence of illegal aliens outweighs the limited intrusion on an individual's privacy that is caused by the checkpoints.[102] As was the case with sobriety checkpoints, the effectiveness of the fixed immigration checkpoint in *United States v. Martinez-Fuerte*[103] was a critical aspect of its reasonableness. There, the record established a "rather complete picture of the effectiveness of the . . . checkpoint."[104]

By way of contrast, in *Delaware v. Prouse*,[105] the Supreme Court disapproved of random stops made by Delaware Highway Patrol officers to apprehend unlicensed drivers and unsafe vehicles, since there was no empirical evidence that such stops would effectively promote roadway

in *Sitz* was twenty-five seconds. *Id*. at 456. By way of contrast, the delay in the random illegal immigrant checkpoint upheld by the Court in *Martinez-Fuerte* was three to five minutes. United States v. Martinez-Fuerte, 428 U.S. 543, 545-548 (1976). The federal courts have also concluded that routine traffic stops lasting no more than fifteen minutes are not unreasonable. *E.g*., Merrett v. Moore, 58 F.3d 1547, 1553 (11th Cir. 1995).

97. Sobriety checkpoints clearly have been effective in reducing alcohol-related traffic fatalities and accidents. *See* CENTER FOR DISEASE CONTROL, RESEARCH UPDATE: SOBRIETY CHECKPOINTS ARE EFFECTIVE IN REDUCING ALCOHOL-RELATED CRASHES (2002), *available at* http://www.cdc.gov/MotorVehicleSafety/Impaired_Driving/checkpoint.html (finding that alcohol-related traffic deaths reduced by 20% in states that implemented sobriety checkpoints as compared to those that did not); *see also* PUBLIC HEALTH LAW RESEARCH, SELECTIVE BREATH TESTING SOBRIETY CHECKPOINTS (2009), *available at* http://publichealthlawresearch.org/public-health-topics/injury-prevention-evidence-briefs/motor-vehicles-and-alcohol/evidence-brief/sel.

98. *Sitz*, 496 U.S. at 451 ("[A]lcohol-related death and mutilation on the Nation's roads are legion."); *see also* 4 W. LaFave, *supra* note 49, at §10.8(d) ("Drunk drivers cause an annual death toll of over 25,000 and in the same time span cause nearly one million personal injuries and more than five billion dollars in property damage.").

99. *Sitz,* 496 U.S. at 451 ("No one can seriously dispute the magnitude of the drunken driving problem or the States' interest in eradicating it.").

100. *Id.*; *see also* Delaware v. Prouse, 440 U.S. 648, 658, 663 (1979) (holding that a State's "vital interest" in ensuring "highway safety" could also support "questioning of all oncoming traffic at roadblock-type stops").

101. *Martinez-Fuerte*, 428 U.S. at 562 ("Accordingly, we hold that the stops and questioning at issue may be made in the absence of any individualized suspicion at reasonably located checkpoints.").

102. *Cf*. *Sitz,* 496 U.S. at 453 ("The intrusion resulting from the brief stop at the sobriety checkpoint is for constitutional purposes indistinguishable from the checkpoint stops we upheld in *Martinez–Fuerte*."); *see also* 5 LaFave, *supra* note 49, at §10.8(d).

103. 428 U.S. at 543.

104. *Id.* at 554.

105. 440 U.S. at 648.

safety.[106] Indeed, the Court stated that "common sense" indicated that the "percentage of all drivers on the road who were driving without a license was very small and that the number of licensed drivers who will be stopped in order to find one unlicensed operator will be large indeed."[107]

In addition to the effectiveness requirement, another key aspect of the Supreme Court's endorsement of fixed checkpoints is that they must be carried out pursuant to a "plan embodying explicit, neutral limitations on the conduct of individual officers."[108] The officer's "discretion" at the checkpoint was, therefore, one of the primary factors that led to the condemnation of the roving checkpoints for aliens in *Almeida-Sanchez v. United States.*[109] On the other hand, the Supreme Court upheld the use of the fixed immigration checkpoints in *United States v. Martinez-Fuerte* because they involved "less discretionary enforcement activity," were conducted in a "regularized manner," and reassured law-abiding motorists that the stops were "duly authorized" and served the "public interest."[110] Finally, the locations of the checkpoints were not selected "by officers in the field, but by officials responsible for making overall decisions as to the most effective allocation of limited enforcement resources."[111]

One aspect of the sobriety and immigration checkpoint cases that should be further considered in regard to their application to virtual checkpoints in cyberspace, however, is the public nature of the checkpoints, as well as the public notice that accompanies them. Generally speaking, citizens are notified of the existence and location of these checkpoints and are able to observe the manner in which the checkpoints are administered.[112] While the specific persons who are stopped at such checkpoints may not be

106. *Id*. at 659-661.

107. *Id*. at 659-600. However, while random stops that involve "standardless and unconstrained discretion" are constitutionally suspect, the Supreme Court did not "cast doubt on the permissibility of roadside truck weigh-stations and inspection checkpoints, at which some vehicles may be subject to further detention for safety and regulatory inspection." *Id*. at 661, 663 n. 26; *see also* City of Indianapolis v. Edmond, 531 U.S. 32, 47 (2000) (holding that the constitutionality of checkpoint programs depends on a "balancing of the competing interests at stake and the effectiveness of the program").

108. *Edmond*, 531 U.S. at 49.

109. 413 U.S. 266 (1973); *see also* United States v. Ortiz, 422 U.S. 891, 895 (1975) ("Moreover we are not persuaded that the checkpoint limits to any meaningful extent the officer's discretion to select cars for search.").

110. United States v. Martinez-Fuerte, 428 U.S. 543, 559 (1976).

111. *Id*.

112. *See* Michigan Dept. of State Police v. Sitz, 496 U.S. 444, 453 (1990) ("'[T]he circumstances surrounding a checkpoint stop and search are far less intrusive than those attending a roving-patrol stop. Roving patrols often operate at night on seldom-traveled roads, and their approach may frighten motorists. At traffic checkpoints the motorist can see that other vehicles are being stopped, he can see visible signs of the officers' authority, and he is much less likely to be frightened or annoyed by the intrusion.") (quoting *Ortiz*, 422 U.S. at 894-895 (1975)).

personally aware of the existence of the checkpoints until they arrive at them, the public nature of the checkpoints has been a factor that the Supreme Court has noted.[113]

On the other hand, this factor should not be dispositive of the constitutionality of a virtual checkpoint in cyberspace. Indeed, the virtual checkpoints on the nation's information superhighway that are the subject of this article would only be established after extensive public debate, and only after congressional approval. In such circumstances, it is possible to accommodate public and private interests, and to properly cabin the scope of the government's conduct. If the virtual checkpoints in cyberspace involve minimal intrusion, are reasonably effective, and are administered in a regularized manner that limits the discretion of those administering them,[114] and if their programmatic purpose is to minimize the cybersecurity risks to the nation's critical infrastructure and key resources and not ordinary crime control,[115] then they can be constitutional.

C. Searches by Narcotics-Detection Dogs

Cases that concern searches by narcotics-detection dogs also provide an important analytical framework for determining whether digital scans that initially do not involve human review implicate protected Fourth Amendment interests. These cases are sometimes referred to as the "binary" search cases because narcotics-detection dogs provide only a "positive or negative response" as to the presence of illegal narcotics.[116] Two major Supreme Court cases have addressed the relationship between

113. *See Martinez-Fuerte*, 422 U.S. at 559 ("Motorists using these highways are not taken by surprise as they know, or may obtain knowledge of, the location of the checkpoints and will not be stopped elsewhere. Second, checkpoint operations both appear to and actually involve less discretionary enforcement activity. The regularized manner in which established checkpoints are operated is visible evidence, reassuring to law-abiding motorists, that the stops are duly authorized and believed to serve the public interest.").

114. Delaware v. Prouse, 440 U.S. 648, 663 (1979) ("This holding does not preclude the State of Delaware or other States from developing methods for spot checks that . . . do not involve the unconstrained exercise of discretion. Questioning of all oncoming traffic at roadblock-type stops is one possible alternative.").

115. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing."); *id*. at 44 ("We decline to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes.").

116. *E.g*., Ric Simmons, *The Two Unanswered Questions of Illinois v. Caballes: How to Make the World Safe for Binary Searches*, 80 TUL. L. REV. 411, 413 (2005). According to Professor Simmons, the first reported case to use the term "binary" in connection with a dog sniff was United States v. Colyer, 878 F. 2d 469, 474 (D.C. Cir. 1989) ("As in *Place*, the driving force behind *Jacobsen* was the recognition that because of the binary nature of the information disclosed by the sniff, no legitimately private information is revealed: That is, 'the governmental conduct could reveal nothing about noncontraband items.'") (citation omitted).

the Fourth Amendment and narcotics-detection dogs: *Illinois v. Caballes*[117] and *United States v. Place*.[118] In *Caballes*, an Illinois State Trooper stopped Caballes for speeding on an interstate highway, and another trooper responded to the scene.[119] While the first trooper was in the process of writing a traffic-related warning ticket, the second trooper accompanied his dog around Caballes' car, and when the "dog alerted" near the trunk, the resulting search led to the discovery of marijuana.[120] After concluding that the initial stop was lawful, the Supreme Court went on to analyze whether the dog sniff "unreasonably infringe[d] interests protected by the Constitution."[121] The Court concluded that a dog sniff conducted during a lawful traffic stop "does not violate the Fourth Amendment" because it "reveals no information other than the location of a substance that no individual has any right to possess."[122] Thus, the non-human, binary intrusion did "not rise to the level of a constitutionally cognizable infringement."[123]

The majority in *Caballes* found support for its decision in the Court's 1983 decision in *United States v. Place.*[124] Place had engaged in suspicious behavior as he waited in a ticket line at the Miami International Airport and after he arrived in New York. When Place refused to consent to a search of his luggage, the agents in New York took his bags and subjected them to a "sniff test" by a trained narcotics-detection dog. The dog reacted positively, which led to a search warrant and the discovery of cocaine.[125] Writing for the majority, Justice Sandra Day O'Connor stated that "given the enforcement problems associated with the detection of narcotics trafficking and the minimal intrusion that a properly limited detention [of personal luggage] would entail, the Fourth Amendment does not prohibit such a detention."[126] The Court noted that the use of the narcotics-detection dog was "*sui generis*" since the court was aware of "no other investigative technique that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure;"[127] that is, the canine sniff only revealed the "presence or absence of narcotics,

117. 543 U.S. 405 (2005).

118. 462 U.S. 696 (1983).

119. *Caballes*, 543 U.S. at 406.

120. *Id*.

121. *Id.* at 407 ("[A] seizure that is lawful at its inception can violate the Fourth Amendment if its manner of execution unreasonably infringes interests protected by the Constitution.").

122. *Id.* at 410.

123. *Id*. at 409.

124. 462 U.S. 696 (1983).

125. *Id*. at 700.

126. *Id*. at 698.

127. *Id*. at 707.

a contraband item."[128] Thus, the Court concluded that a "well-trained narcotics detection dog . . . does not expose noncontraband items that otherwise would remain hidden from public view."[129] Although the seizure in *Place* exceeded the "bounds of a permissible investigative detention of the luggage,"[130] the Court stated that the dog sniff of Place's personal luggage at the airport "did not constitute a 'search' within the meaning of the Fourth Amendment."[131]

Although it is not a dog-sniff case, *Kyllo v. United States*[132] must be considered in regard to the issue of whether digital scans at virtual checkpoints that initially involve no human review would run afoul of the Fourth Amendment. In *Kyllo*, government agents had used a thermal-imaging detection device to measure the temperature inside of the defendant's garage while they were sitting in a car parked on a public street.[133] The purpose of the device was to detect the cultivation of marijuana. When the device showed that the garage was atypically warm, the agents suspected that Kyllo was using it as a marijuana greenhouse. In finding that the use of the device required a warrant, the Supreme Court noted the fact that the search took place in a home, a location where Fourth Amendment protection from the government has historically been the greatest,[134] as well as the fact that the search was not strictly binary in nature.[135] Indeed, writing for the majority, Justice Antonin Scalia noted that the thermal-imaging detection device was also capable of detecting lawful activity, such as "at what hour each night the lady of the house takes her daily sauna and bath."[136]

128. *Id*.

129. *Id*.; *see also* City of Indianapolis v. Edmond, 531 U.S. 32, 40 (2000) (noting that a dog sniff is "not designed to disclose any information other than the presence or absence of narcotics").

130. *Place*, 462 U.S. at 698.

131. *Id*. at 707.

132. 533 U.S. 27 (2001).

133. *Id.* at 29-30.

134. *Id*.; *see also* Payton v. New York, 445 U.S. 573, 586-87 (1980) ("It is a 'basic principal of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable.") (footnote omitted). *See generally* David E. Steinberg, *Restoring the Fourth Amendment: The Original Understanding Revisited*, 33 HASTINGS CONST. L. Q. 47 (2005).

135. Justice Souter was concerned with "false positives" that revealed "undisclosed facts about private enclosures, [which would then be] used to justify a further and complete search of the enclosed area." Illinois v. Caballes, 543 U.S. 405, 412-414 (2005) (Souter, J., dissenting). Justice Ginsburg was also concerned that the scope of the initial stop can become unconstitutionally "broader" if it is not linked to a *Terry*-analysis. *See id*. at 419-421 (Ginsburg, J., dissenting).

136. *Kyllo*, 533 U.S. at 38 ("The [imaging device] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath – a detail that many would consider 'intimate.'").

Some commentators see "tension between the *Kyllo* rule and the logic permitting suspicionless dog sniffs."[137] Others stress that it is critical to "unlink the seizure question from the search question," noting that "if the absence of physical intrusion is seen as a critical component of the search evaluation, then new technologies (and many existing technologies) that produce nonbinary results could conceivably be accepted merely because they are completely noninvasive."[138] Taken together, however, *Caballes, Place, and Kyllo* provide important touchstones that limit the scope of a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements. First, to the extent that the government may be examining "metadata," which includes Internet Protocol addresses and other non-content information,[139] it is fairly well-settled that metadata does not receive the same level of privacy protection which is afforded to the contents of electronic (or wire) communications.[140] Second, under the approach discussed in this article, the digital scans of the contents of such communications would initially involve no human review and would only be looking for malicious digital "signatures."[141] Finally, such scans would be binary, and further analysis would only take place if there was a reasonable basis to believe that a malicious digital code may be present.[142]

Under these circumstances, reasonable and limited digital scans at virtual checkpoints in cyberspace would be "justified at their inception"[143] and would not unreasonably intrude upon protected Fourth Amendment interests. While legislative exceptions may be needed for certain persons, such as individuals designing computer intrusion and detection technology, that does not detract from the support that these cases provide to, and how they cabin, a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements.

137. *See Summary of Supreme Court's 2004 Term: The Fourth Amendment – Canine Sniff*, 119 HARV. L. REV. 179, 184 (2004).

138. *See* Simmons, *supra* note 116, at 438-439.

139. *See* Kerr, *supra* note 1, at 1019 (discussing the "content/non-content" line of cases).

140. See Goldsmith, *supra* note 27, at 11 n. 31 and accompanying text (citing Smith v. Maryland, 442 U.S. 735, 743-44 (1979); Quon v. Arch Wireless Co., Inc., 529 F.3d 892, 904-05 (9th Cir. 2008); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)).

141. *See* OLC Legal Issues Memorandum, *supra* note 9, at 3.

142. *See infra* notes 156-163 and accompanying text for a discussion of a cyber-*Terry* stop.

143. *Cf.* O'Connor v. Ortega, 480 U.S. 709, 725 (1987) (plurality) (holding that a search must be "justified at its inception" and "permissible in its scope").

D. Screening Searches at Airport Security Checkpoints

Screening searches that are conducted at airport security checkpoints also provide important limitations on the scope of a cybersecurity exception. Airport screening searches have been upheld because they are "conducted as part of a general regulatory scheme in furtherance of an administrative purpose; namely, to prevent the carrying of weapons or explosives aboard aircrafts, and thereby to prevent hijackings."[144] Indeed, at the present time, "all luggage that goes onto a plane [may be screened] to ensure that it does not contain any explosive devices or other items that would threaten the safety of the plane."[145] As the Ninth Circuit has noted, the "essential purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them, but to deter persons carrying such material from seeking to board at all."[146] As long as the "programmatic purpose"[147] motivating the search is not "a criminal investigatory purpose," it is "justified under an administrative search rationale."[148]

To meet the Fourth Amendment's reasonableness test, airport security screening searches must be "limited to searches for guns or explosives, and . . . no more burdensome than necessary to achieve that objective."[149] The federal courts have noted that airline passengers choose to fly on airplanes, and have been notified of the fact that they and their possessions will be subjected to a search for weapons and explosives.[150] As a result, the

144. United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973). *See generally* 5 LaFave, *supra* note 49, at §10.6(c).

145. United States v. McCarty, 648 F.3d 820, 824 (9th Cir. 2011) ("[The Transportation Security Administration] screens all luggage that goes onto a plane to ensure it does not contain any explosive devices or other items that would threaten the safety of the plane. One method of screening is through an x-ray device such as the CTX machine used here, which can identify potential safety risks or dense items in luggage that require further inspection."). Federal law authorizes Transportation Security Administration agents to searches entire bags for explosives and other safety hazards. *See* 49 U.S.C. §44901 (2006); 49 C.F.R. §1540.111(c) (2006).

146. *Davis*, 482 F.2d at 913.

147. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 47 (2000).

148. United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1246 n. 5 (9th Cir. 1989); *cf*. *Edmond,* 531 U.S. at 41 ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.").

149. *$124,570 U.S. Currency*, 873 F.2d at 1245.

150. 5 LaFave, *supra* note 49, at §10.6(e) (collecting cases and noting that passengers are "forewarned by the signs posted in the airport, by the announcement made there over the public address system, or by observation of the search procedures while in the checkpoint line"). While notice to the public and the pervasiveness of government activity can reduce reasonable expectations of privacy, some scholars emphasize that ultimately this question is a "value judgment," and "if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society." Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

screening searches at airport security checkpoints do not require individualized suspicion to be constitutional, despite the fact they could "lead to discovery of contraband and apprehension of law violators."[151]

Of course, when all passengers are randomly searched,[152] the decision to search is not subject to the unfettered discretion of the officer in the field. All persons passing through airport security checkpoints are subjected to searches through "established procedures, and those conducting the searches play no part in determining who will choose to include themselves within the group of persons to be screened."[153] Moreover, because screening searches at airport security checkpoints are only as intrusive as necessary to accomplish their non-law enforcement, protective purpose, the searches are reasonable.[154] As a result, although airport security checkpoints may not be a perfect analog for virtual checkpoints in cyberspace, they nonetheless inform the scope of a cybersecurity exception to the Fourth Amendment; that is, the initial digital scans for malicious digital codes should be conducted through "established procedures" and should be no more intrusive than is necessary "in the light of the current technology."[155]

E. Terry-Stops

While the "stop and frisk" cases do not fall into the "administrative search" or the "special needs" category of cases, *Terry v. Ohio*[156] and its progeny provide an important additional analytical framework to evaluate protective actions that the government should be able to take in cyberspace. The facts in *Terry* are fairly straightforward. Two men were acting

151. *Davis*, 482 F.2d at 908 ("Of course, routine airport screening searches will lead to discovery of contraband and apprehension of law violators. This practical consequence does not alter the essentially administrative nature of the screening process, however, or render the searches unconstitutional.").

152. Some passengers are randomly selected for additional screening "regardless of whether or not the x-ray luggage scan reveals something suspicious." United States v. Marquez, 410 F.3d 612, 614 (9th Cir. 2005).

153. 5 LaFave, *supra* note 49, at §10.6(c). The "randomness of the selection for the additional screening procedure arguably increases the deterrent effects of airport screening procedures because potential passengers may be influenced by their knowledge that they may be subject to random, more thorough screening procedures." *Marquez*, 410 F.3d at 614.

154. *Cf. $124,570 U.S. Currency*, 873 F.2d at 1245-46 (noting that too "close [of a] working relationship" with "law enforcement authorities" could alter "the calculus" by which airport security searches have been upheld).

155. *See Davis*, 482 F.2d at 913 ("In light of that need, a screening of passengers and of the articles that will be accessible to them in flight does not exceed constitutional limitations provided that the screening process is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to fly.").

156. 392 U.S. 1 (1968).

suspiciously on a street corner in downtown Cleveland and talking with a third man, and the police concluded that they were "casing" a store in preparation for an armed robbery.[157] The officer confronted the men, identified himself, and began to question them. One of the men mumbled something and the officer then spun Terry around and began a pat down. After feeling the outline of a gun, the officer removed the weapon. A pat down of the second man also revealed a concealed weapon.[158]

When the case reached the Supreme Court, the question was "whether it is always unreasonable for a policeman to seize a person and subject him to a limited search for weapons unless there is probable cause for an arrest."[159] After "balancing the need to search against the invasion which the search entails," the Court answered the question in the negative, and concluded that law enforcement officers are only required to establish "reasonable suspicion" to justify a brief detention and protective pat down of the outer clothing for weapons.[160] The Supreme Court then articulated the reasonable suspicion standard, holding that it exists when a policeman can point to "specific and articulable facts which, taken together with rational inferences from those facts," lead the officer "reasonably to conclude in light of his experience that criminal activity may be afoot."[161]

If a digital scan at a virtual checkpoint in cyberspace leads computer intrusion and detection technology to a reasonable belief that a malicious digital code may be present in an electronic (or wire) communication, then *Terry*'s reasonable suspicion standard and the compelling governmental interest to prevent such a code from harming the nation's critical infrastructure and key resources should permit the government to conduct a cyber-*Terry* stop and temporarily "detain" the communication for further analysis. Such "detention" and further analysis of the communication should last, however, "no longer than is necessary to effectuate the purpose of the stop."[162] Thus, the scope of any cyber-*Terry* stop should be "'strictly tied to and justified by' the circumstances which rendered its initiation permissible."[163]

157. *Id*. at 5-8.

158. *Id*.

159. *Id*. at 15.

160. *Id*. at 20, 27 (holding that a stop and frisk is not unreasonable so long as the officer had a "reason to believe that he is dealing with an armed and dangerous individual, regardless of whether he has probable cause to arrest the individual for a crime").

161. *Id*. at 21, 30. *See generally* 4 LaFave, *supra* note 49, at §9.1(b)-(e).

162. Florida v. Royer, 460 U.S. 491, 500 (1983) ("This much, however, is clear: an investigative detention must be temporary and last no longer than is necessary to effectuate the purpose of the stop. Similarly, the investigative methods employed should be the least intrusive means reasonably available to verify or dispel the officer's suspicion in a short period of time."); *see also* United States v. Place, 462 U.S. 696, 709 (1983) (noting the importance of the delay caused by the seizure).

163. *Terry*, 392 U.S. at 19 (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring).

F. The Government's Quarantine Authority

The legal framework which governs the government's quarantine and isolation[164] authority with respect to communicable diseases that pose a risk to public health has direct application to the legal framework that should govern the government's ability to protect the nation from malicious digital codes that pose a risk to critical infrastructure and key resources. First, it is clear that the federal government's quarantine authority is at its "zenith at the international border."[165] Indeed, the Department of Homeland Security has the authority to prevent the admission into the United States of any alien "who is determined (in accordance with regulations prescribed by the Secretary of Health and Human Services) to have a communicable disease of public health significance."[166] Moreover, such aliens may be temporarily detained at ports of entry for the purpose of determining whether they are inadmissible by virtue of having a communicable disease of "public health significance."[167]

The ability to quarantine persons travelling domestically within the United States is primarily based upon the "police power" of a State.[168] The Supreme Court has recognized for more than a century that a State has the power to enact "reasonable regulations" to detain and quarantine individuals who pose a threat to "the public health and the public safety."[169] The federal government, however, also has some domestic quarantine

164. Quarantine and isolation are often used "interchangeably" but refer to different individuals in the physical world. *See* Kathleen Swendiman & Jennifer K. Elsea, *Federal and State Quarantine and Isolation Authority* (Cong. Res. Service RL33201), Jan. 23, 2007, at 2. Quarantine refers to individuals who have been exposed to communicable diseases but are "not yet ill," and isolation refers to individuals are already "infected." *Id*; *see also* LAWRENCE O. GOSTIN, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 209-210 (2d ed. 2008) (discussing the differences between quarantine and isolation). This article uses the term quarantine to generically refer to any remedial action that can be taken by the government against a communicable disease in the physical world or a malicious digital code in cyberspace.

165. United States v. Flores-Montano, 541 U.S. 149, 152 (2004) ("The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border."); *see also* 42 U.S.C. §264(a)-(c) (2006); 42 C.F.R. pt. 71 (2005).

166. 8 U.S.C. §1182(f) (2006); *see also* 42 U.S.C. §265 (2006); 42 C.F.R. pt. 71 (2005).

167. 8 U.S.C. §1182(a)(1) (2006); *see also* 8 U.S.C §1222(a) (2006); 42 U.S.C. §252 (2006); 42 C.F.R. pt. 34 (2008).

168. Jacobson v. Massachusetts, 197 U.S. 11, 24-25 (1905) ("The authority of the state to enact this statute is to be referred to what is commonly called the police power, a power which the state did not surrender when becoming a member of the Union under the Constitution."); *see also* U.S. CONST. amend X. ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.").

169. *Jacobson*, 197 U.S. at 25; *id*. (noting that the court has "distinctly recognized the authority of the state to enact quarantine laws and 'health laws of every description'") (citation omitted).

authority. For example, the Surgeon General, with the approval of the Secretary of Health and Human Services, has the authority to make and enforce quarantine regulations that are "necessary to prevent the introduction, transmission, or spread of communicable diseases."[170] Although such diseases must be identified by the President, pursuant to a number of executive orders, several communicable diseases that authorize the quarantine of individuals have been identified.[171] Federal quarantine regulations also authorize the apprehension and examination of "any individual reasonably believed to be infected with a communicable disease in a qualifying stage," if the individual is "moving or about to move from a State to another State," or is "a probable source of infection to individuals who, while infected with such diseases in a qualifying stage, will be moving from a State to another State."[172]

Other statutes and regulations also provide authority to quarantine individuals and take remedial actions. For example, the Comprehensive Environmental Response, Compensation, and Liability Act of 1980[173] provides the federal government with the ability to engage in "removal" and "remedial" actions to prevent the spread of "hazardous" substances.[174] Such actions include those that "may be necessary to prevent, minimize, or mitigate damage to the public health or welfare or to the environment."[175] The statute also provides that the President may, "after notice to the affected State," take other action "including, but not limited to, issuing such orders as may be necessary to protect public health and welfare and the environment."[176]

The federal government also has the authority to assist state authorities in enforcing a state's quarantine.[177] Indeed, a quarantine may be enforced where it "can be demonstrated that unlimited travel to the area would directly and materially interfere with the safety and welfare of the area or the Nation as a whole."[178] However, a state's quarantine law must not "unreasonably burden or

170. 42 U.S.C. §264(a) (2006); *see also* 42 C.F.R. pt. 70 (2005).

171. *See* 42 U.S.C. §264(b) (2006); Exec. Order No. 13,925, 68 Fed. Reg. 17, 255 (Apr. 4, 2003); Exec. Order No. 13,375, 70 Fed. Reg. 17, 299 (Apr. 1, 2005).

172. 42 U.S.C. §264(d) (2006). *See* 42 C.F.R. pt. 70 (2005).

173. Pub. L. No. 96-510, 94 Stat. 2767 (codified as amended at 42 U.S.C. §§9601-9675) (2006).

174. 42 U.S.C. §9604(a)(1) (2006).

175. 42 U.S.C. §9601(23) (2006).

176. 42 U.S.C. §9606(a) (2006). Similarly, the Commissioner of the Food and Drug Administration can take measures to prevent the spread of communicable diseases from one state or possession into another in the event that measures taken by state or local authorities are inadequate. *See* 21 C.F.R. pt. 1240 (2011). The Director of the Centers for Disease Control and Prevention also can take additional measures to "prevent" the "spread of the diseases as he/she deems reasonably necessary." 42 C.F.R. pt. 70.2 (2005).

177. *See* 42 U.S.C. §243(a) (2006); 42 U.S.C. §§5170, 5192-5193, 5195a (2006).

178. Zemel v. Rusk, 381 U.S. 1, 15-16 (1965); *see also* Compagnie Francaise v. State Board of Health, 186 U.S. 380, 397 (1902) (holding that a state law that regulated the

restrict" a person's constitutional right to travel.[179] Thus, the individual must actually pose a risk to public health, and the quarantine may not be imposed in a manner that deprives an individual of his constitutional rights to equal protection and due process.[180] Quarantines must therefore be conducted in accordance with an individual's substantive and procedural due process rights, and in the least restrictive manner as reasonably possible under the circumstances.[181]

Based on the foregoing, it is clear that the legal framework that governs the government's ability to take remedial actions against persons who pose a health risk as a result of a communicable disease in the physical world informs the legal framework that can be constructed to enable the government to take remedial actions against malicious digital codes in

introduction of persons and property into a district infested with contagious or infectious diseases was "not repugnant to the Constitution of the United States"); Louisiana v. Mathews, 427 F. Supp. 174, 176 (D. La. 1977) ("Congress has granted broad, flexible powers to federal health authorities who must use their judgment in attempting to protect the public against the spread of communicable disease.").

179. *See* Shapiro v. Thompson, 394 U.S. 618, 629 (1969) ("This Court long ago recognized that the nature of our Federal Union and our constitutional concepts of personal liberty unite to require that all citizens be free to travel throughout the length and breadth of our land uninhibited by statutes, rules, or regulations which unreasonably burden or restrict this movement."). It should be noted that a quarantined individual has the ability to petition a federal court for a writ of habeas corpus pursuant to 28 U.S.C. §2241 (2006).

180. *Compare* Smith v. Emery, 42 N.Y.S. 258, 260 (1896) ("The mere possibility that persons might have been exposed to such disease is not sufficient, but they must 'have been exposed to it, and the conditions actually exist for a communication of the contagion.'") (citation omitted), *with* People *ex rel*. Barmore v. Robertson, 134 N.E. 815, 819 (Ill. 1922) ("It is not necessary that one be actually sick . . . in order that the health authorities have the right to restrain his liberties by quarantine regulations. Quarantine . . . is the method used to confine the disease within the person in whom it is detected, or to prevent a healthy person from contracting the infection."), *and* Arkansas v. Snow, 324 S.W.2d 532, 534 (Ark. 1959) (record indicates a "probability that appellee is a very sick person who stubbornly refuses to allow treatment and is probably a source of danger to those around him"); *compare* Wong Wai v. Williamson, 103 F. 1, 9 (N.D. Cal. 1900) (overturning quarantine regulations during a bubonic plaque that were "directed against the Asiatic race exclusively, and by name"), *with* Greene v. Edwards, 263 S.E.2d 661, 663-664 (W. Va. 1980) (overturning a quarantine law because it failed to accord "procedural due process"), *and Ex parte* Hardcastle, 208 S.W. 531, 531 (Tex. Crim. App. 1919) ("The law denies to no one restrained of his liberty without a hearing the right to prove in some tribunal that the facts justifying his restraint do not exist."). Some scholars have also suggested additional conditions, including that quarantines must be "reasonable and effective." *See* Lawrence O. Gostin & Benjamin E. Berkman, *Pandemic Influence, Ethics, Law and the Public's Health*, 59 ADMIN. L. REV. 121, 147 (2007).

181. *See* Jacobson v. Massachusetts, 197 U.S. 11, 18 (1905) (holding that the state's implementation of quarantine laws must neither be arbitrary nor capricious); *id*. at 25 (noting that while the "mode or manner" in which state and local authorities implement quarantine laws is within the discretion of the state, "no rule prescribed by a state, nor any regulation adopted by a local governmental agency acting under the sanction of state legislation, shall contravene the Constitution of the United States, nor infringe any right granted or secured by that instrument").

cyberspace. Among other things, the government's actions in cyberspace should be necessary, the least restrictive as reasonably possible under the circumstances and in light of existing technology, and imposed in a reasonably effective manner to ensure equal protection and due process. While it may be necessary for Executive orders and a regulatory scheme to be promulgated, that does not undermine the constitutional support that exists for a legal regime that will enable the government to protect the "safety and welfare" of the nation's critical infrastructure and key resources from malicious digital codes.[182]

III. LESSONS FROM THE PHYSICAL WORLD AND PROPOSED LEGISLATION

Some courts and commentators have searched for the "'right' analogy to mediate new technology and old rules."[183] Finding such analogies, however, can prove to be illusive because physical world analogies frequently break down in cyberspace when they are scrutinized closely. Others have stated that "new technologies should lead us to look more closely at just what values the Constitution seeks to preserve."[184] While both of these approaches are important, as the foregoing discussion demonstrates, applying the Fourth Amendment correctly to new technologies is also dependent upon the use of the appropriate lens (or framework). Indeed, even if one could find the right analogy and used a values-based approach, one would nonetheless reach an erroneous result if one did not focus on the issues with the correct Fourth Amendment lens. The "lens" method of legal analysis is based upon the premise that one has a better chance of arriving at the correct result only if one begins the analysis with the correct lens.[185] While adherence to underlying values is essential and while policy choices may alter results, if one begins the

182. *See* Zemel v. Rusk, 381 U.S. 1, 15-16 (1965) (noting that unlimited travel "would directly and materially interfere with the safety and welfare of the . . . Nation as a whole").

183. *See* Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1319 (2011).

184. Laurence H. Tribe, Harvard Law School, Keynote at the 1991 Computers Freedom and Privacy Conference, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier* (1991), *available at* http://epic.org/free_speech/tribe.html. *See* Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 49 (2002) (arguing that the Supreme Court should address new technologies by enunciating an "expansive, value-based theory of the scope of the Fourth Amendment"); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 165, 222 (1999) ("We must always adopt readings of the Constitution that preserve its original values.").

185. Sometimes the correct lens is a "hybrid" lens. *See* Scott J. Glick, *FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security*, 1 HARV. NAT'L SEC. J. 87, 110 (2010) ("Foreign intelligence and law enforcement investigations to protect national security [are] 'hybrid' in nature.").

analysis with the wrong lens, there is a greater chance that when doctrinal principles and values are applied, one will reach erroneous conclusions. Here, it is a protective lens, as opposed to a criminal, intelligence, or military lens, that strongly supports the existence of a cybersecurity exception to the Fourth Amendment's warrant and individualized suspicion requirements.

This cybersecurity exception, however, is a limited one and is appropriately informed by the doctrinal limitations of the special needs and administrative search cases, as well as by the other legal frameworks from the physical world discussed above. While individual aspects of these legal frameworks may not map perfectly to cyberspace, when viewed together, they inexorably lead to the conclusion that reasonable and limited digital scans at virtual checkpoints in cyberspace can be constitutional – notwithstanding the lack of individualized suspicion or a court order – because the programmatic purpose of those scans is to identify malicious digital codes that may be attacking the nation's critical infrastructure and key resources. Moreover, because these digital scans are focused only on identifying the presence or absence of malicious digital codes, there is minimal risk of unwarranted invasions of privacy, particularly as compared to physical searches by law enforcement officers at international borders, sobriety checkpoints, airports, or even in subway stations.[186] Thus, computer intrusion and detection technology that is binary and does not initially expose the contents of electronic (or wire) communications to human review can be a constitutional and effective means to protect the nation's critical infrastructure and key resources.[187]

Addressing the constitutional question, however, does not end the inquiry. Unless a specific statutory exception exists, Title III makes it unlawful to "intentionally intercept" any "wire . . . or electronic communication."[188] While the "prior consent" exception is enumerated in

186. Following a series of coordinated attacks on the London Subway system, New York instituted a security checkpoint program at selected subway stations to systematically search the bags of subway riders for explosives. The Second Circuit upheld the checkpoints under the "special needs" framework. *See* MacWade v. Kelly, 460 F.3d 260, 268 (2d Cir. 2006). *See generally* Case Comment, *Second Circuit Holds New York City Subway Searches Constitutional Under Special Needs Doctrine*, 120 HARV. L. REV. 635 (2006).

187. *Cf. In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions.").

188. 18 U.S.C. §2511(1) (2006) ("Except as otherwise specifically provided in this chapter any person who . . . intentionally intercepts . . . any wire . . . or electronic communication" violates Title III."). FISA also makes it unlawful to intercept communications without an "express statutory authorization." *See* 50 U.S.C. §1809 (2006); *id*. §1812 (exclusivity provision).

the statute,[189] and while an Internet service provider may intercept Internet communications to protect its property,[190] neither of these statutory exceptions is sufficiently broad to encompass all of the virtual points in cyberspace where the government can and should be detecting the presence of malicious digital codes that may be attacking critical infrastructure and key resources.[191]

As a result, while the foregoing discussion demonstrates that fairly well-established Fourth Amendment doctrines from the physical world provide a solid *constitutional* foundation for reasonable and limited digital scans for malicious codes at virtual checkpoints in cyberspace, an explicit *statutory* cybersecurity exception is needed in Title III. Such an exception could read along the following lines:

> Notwithstanding any other law, it shall not be unlawful for an officer, employee, or agent of the United States, or of any State, in the normal course of his official duty, to conduct reasonable and limited digital scans of electronic or wire communications in order to identify, quarantine, or isolate any malicious digital code that may be attacking, has attacked, or is about to attack the critical infrastructure or key resources of the United States or of any State.

In view of the important policy choices[192] that are stake, however, any legislation should be guided by the principles discussed *infra*. Indeed, a free and open Internet is essential to the continued economic vitality of our nation.[193] Thus, in seeking to create a legal framework for protective actions in cyberspace, the government must ensure that it does not unreasonably infringe upon cherished constitutional freedoms and values. As one former Department of Justice Official has noted, expanding a computer intrusion and detection system to the public Internet may very well cause the "Internet culture [to] rise up in revolt."[194] While reasonable people may

189. 18 U.S.C. §2511(1)(c) (2006).

190. *Id.* §2511(2)(a)(i) (2006).

191. *See supra* note 9. *See also* Ellen Nakashima, Internet Carriers Join Forces To Foil Cyberattacks, WASH. POST, June 16, 2011, at A1.

192. For example, Congress may conclude that digital scans should only be permitted in regard to malicious digital codes that may be attacking a limited subset of critical infrastructure and key resources, or that the government should be required to make a showing to a court before setting up virtual checkpoints in cyberspace. *See also* Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 899-903 (2010) (discussing the role of legislatures in deciding what is "reasonable" under the fourth amendment).

193. *See* Nojeim, *supra* note 42, at 119 ("[C]ybersecurity efforts must be carefully tailored in order to preserve privacy, liberty, innovation, and the open nature of the Internet").

194. Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARV. NAT'L SEC. J. 366, 376 (2011). *See* John N. Greer, *Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of*

disagree about whether this overstates the case, any new cybersecurity legal framework must be mindful of the "privacy rights and civil liberties [that are] guaranteed by the Constitution and law."[195] Public debate is therefore critical, particularly in view of the policy choices that are available to the nation's lawmakers, and "[c]oncrete mechanisms to protect privacy and to ensure that the government's search is minimally intrusive and reasonably efficacious"[196] are essential.

New cybersecurity legislation, executive orders, and regulations that authorize the government to use reasonable and limited digital scans at virtual checkpoints in cyberspace, and to take remedial and other actions[197] should therefore be informed by the following:

A. Digital scans at virtual checkpoints in cyberspace should be administered in a regularized, fair and reasonable fashion pursuant to established regulations and procedures which do not permit arbitrary or capricious scanning that is unrelated to the protection of critical infrastructure and key resources;

B. Digital scans should be conducted in the least intrusive means necessary to accomplish their purpose in light of existing technology; that is, they should not initially expose the contents of the communications to human review, and they should be binary and determine whether or not there is a reasonable basis to believe that a malicious digital code may be present;

Privacy Rights and Civil Liberties in Cyberspace, 4 J. NAT'L SECURITY L. & POL'Y 139, 141 (2010) ("Many people are rightly concerned when they hear that intelligence agencies will be more active in cyberspace."); Chertoff, *supra* note 28, at 5 (warning of "dangers" if "the government directly operates civilian domain security, as opposed to simply setting standards for security and enabling private entities to operate the security function in private space").

195. *See* Greer, *supra* note 194, at 139.

196. *See* Goldsmith, *supra* note 27, at 13-15.

197. Of course, sending a malicious digital code to attack critical infrastructure and key resources is a criminal offense. *See* 18 U.S.C. §1030 (2006). As a result, to the extent that forensic examinations and other investigative activities are able to determine the identity of the criminal, under well-established Fourth Amendment principles, the resulting evidence would be the "fruit" of a healthy tree. *Compare* City of Indianapolis v. Edmond, 531 U.S. 32, 48 (2000) ("Our holding also does not impair the ability of police officers to act appropriately upon information that they properly learn during a checkpoint stop justified by a lawful primary purpose, even where such action may result in the arrest of a motorist for an offense unrelated to that purpose."), *with* Wong Sun v. United States, 371 U.S. 471, 487-488 (1963) ("We need not hold that all evidence is 'fruit of the poisonous tree' simply because it would not have come to light but for the illegal actions of the police."). Professor Simmons, however, argues that suspicionless antiterrorism searches should only be permitted pursuant to the special needs doctrine if the fruits of those searches cannot be used as evidence in a criminal prosecution. *See* Simmons, *supra* note 192, at 915-926.

C. Mechanisms should be put in place to ensure that regular government and Congressional oversight exists; that is, the Executive Branch and the Legislative Branch should ensure that the digital scans continue to be necessary in light of the cybersecurity risks, and that they are reasonably accurate and effective at identifying malicious digital codes that have attacked, may be attacking, or are about to attack, critical infrastructure and key resources;[198]

D. If an digital scan leads to a reasonable belief that a malicious digital code may be present, then a cyber-*Terry* stop should take place which enables the government to use the least intrusive means reasonably available, under the circumstances and in light of existing technology, to verify or dispel its belief that a malicious digital code may be present; and

E. Cybersecurity quarantine and related authorities should be promulgated to enable the government to take reasonably effective remedial and other actions against malicious digital codes. Any regulatory scheme, however, should be as minimally restrictive as reasonably possible, under the circumstances and in light of existing technology, to ensure equal protection and due process.[199]

CONCLUSION

The cybersecurity risks to the nation are significant and increasing every day, and unless those risks are minimized, there could be serious and devastating consequences to the nation's critical infrastructure and key resources. As a result, at this moment in time, the nation needs to answer two key "foundational" questions; namely, "what technical tools are the American people comfortable having the government deploy, and what level of government involvement and interaction with the private sector will the people allow."[200] While a sound legal basis exists for the government to use computer intrusion and detection technology to protect its own networks without the need for a court order or individualized suspicion, and while there are several cybersecurity policies that can and should be implemented, new thinking is required if the nation is going to be able to

198. Such mechanisms could include "minimization procedures," "ex post auditing and reporting requirements," and a "sunset provision." *See* Goldsmith, *supra* note 27, at 15-16.

199. Remedial measures could range from the "least invasive (such as stripping off the malicious code) to most intrusive (destroying the communication)." *Id*. at 15.

200. Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 233 (2010).

minimize the cybersecurity risks to our critical infrastructure and key resources, which are primarily owned by the private sector.

When viewed through a protective Fourth Amendment lens, fairly well-established legal frameworks from the physical world can provide a sound doctrinal basis for finding a new cybersecurity exception to the Fourth Amendment's individualized suspicion and warrant requirements. While certain aspects of these legal frameworks may not map perfectly to cyberspace, when viewed together, they strongly support a cybersecurity exception that enables the government to conduct reasonable and limited digital scans at virtual checkpoints in cyberspace to minimize the risks posed by malicious digital codes that may be attacking the nation's critical infrastructure and key resources. Congress should therefore consider and enact sensible new legislation that will allow digital scans at virtual checkpoints and cyber-*Terry* stops to take place within the constitutional framework that has enabled this nation to prosper.