U.N. REGULATION - THE BEST APPROACH TO EFFECTIVE CYBER DEFENSE?

Sarah A. Lafen†

---

† Juris Doctor Candidate, 2018, Syracuse University College of Law. The author would like to thank Professor William C. Snyder for his unparalleled expertise and guidance throughout the process of writing this piece.

I. INTRODUCTION

As a rapidly growing threat and form of warfare, cybersecurity's presence in today's international community demands effective and proactive responses from the public and private sectors – as each sector is affected by such crime.[1] Defending against foreign attacks requires a two-pronged approach and would best be implemented and governed by the United Nations (U.N.) to ensure uniform standards and regulation. First, public private partnerships (PPPs) must reach a level of seamless cooperation within nations in order to most effectively defend against foreign cyberattacks. Second, such defense cannot be accomplished on solely a domestic level. International cooperation, which is essential to defending against foreign cybercrime, can most successfully be accomplished through utilizing the U.N. as the regulating body to set forth specific regulations for nations to follow and utilize to cooperate with each other.

Nations have shown increased efforts to strengthen their domestic cybersecurity departments,[2] and the need for international cooperation within PPPs has been recognized by many as an essential step in effective cyber defense.[3] Integrating these two widely-recognized concepts into one method governed by the U.N. would better regulate cyber defense and ensure a cohesive governing body over this prevalent issue.

---

1. *See* Marthie Grobler et al., *Preparing South Africa for Cyber Crime and Cyber Defense*, 11 SYSTEMICS, CYBERNETICS & INFORMATICS 32, 33 (2013).

2. *National Digital Security Strategy: "A Good Balance Between Security Considerations and Economic Dynamism,"* GOUVERNEMENT.FR (Oct. 19, 2015), *available at* http://www.gouvernement.fr/en/national-digital-security-strategy-a-good-balance-between-security-considerations-and-economic (last visited Apr. 10, 2018) (noting that the French National Cybersecurity Agency 'Anssi' vowed to increase their agents from an initial 100 when the agency was founded in 2009, to 600 agents by 2017).

3. *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models, Intelligence and National Security Alliance* (Nov. 2009), *available at https://www.insaonline.org/wp-content/uploads/2017/04/INSA_AddressingCyber_WP.pdf* (last visited Apr. 10, 2018).

The first section of this note will provide a brief overview of the status of the world in cybersecurity today and will speak briefly to the importance of international agreements. The second section will explore successful versus ineffective collaborations between the public and private sectors, with a close focus on the goals and importance of partnerships as well as common obstacles that both sectors face prior to and after engaging in a partnership. This section will also look into existing cybersecurity bodies of different nations and will analyze successful collaborations along with areas that can be improved upon in order to have a more effective impact on the prevention of foreign cyberattacks. Because defense against foreign cyberattacks cannot be accomplished through domestic measures alone, the third section examines international law's role in cybersecurity, with specific focus on the benefit of international cooperation between nations on a large scale. This section will look into the domestic practices that various countries use to defend against cyberattacks from foreign actors, potential issues with both existing and proposed collaborations, and international law governing public and private sector partnerships. This section also will examine why the U.N. is the most effective body to regulate and govern this cooperation between nations.

II. PUBLIC AND PRIVATE CYBERSECURITY: A BRIEF OVERVIEW

As warfare evolves, cyberattacks, cybercrime, and cyberespionage have become more prevalent and inevitable than ever before. Some nations have publicly declared that cybercrime is a main element of their foreign military strategy.[4] As attractive targets, government systems lure foreign cyber hackers through the very existence of national security secrets and personal identification information.[5] In November 2016, Saudi Arabia's aviation agency was attacked by a foreign actor that sent a virus specifically intended to penetrate government agencies.[6]

Private corporations are also common victims of cyberattacks, regardless of their size or apparent abundance of resources to prevent

4. Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, 1, 5 (2010), *available at* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (last visited Apr. 10, 2018).

5. *Id.*

6. Sewell Chan, Cyberattacks Strike Saudi Arabia, Harming Aviation Agency, N.Y. TIMES (Dec. 1, 2016), *available at* https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html?_r=0 (last visited Apr. 10, 2018).

such attacks. Within the past five years, Staples, Home Depot, and JPMorgan Chase have all been victims of cyberattacks.[7] A single data breach reportedly costs U.S. companies each approximately $500,000.[8] As a result of successful hacks, the public images of these corporations suffer, and a large range of their sensitive information is compromised including product ideas, merger and acquisition information, corporate strategy, employment records, customer records, and financial data.[9] Further, smaller businesses are becoming more prone to attacks because they are typically less prepared and able to defend themselves than governments and larger businesses.[10]

Commonly accused offenders of cyberattacks on both foreign nations and private entities include China, Israel, North Korea, Iran, Russia, and the United States (U.S.).[11]

III. COLLABORATION BETWEEN THE PUBLIC AND PRIVATE SECTOR

Collaboration between the public and private sectors is a vital step in securing effective countermeasures against cyberattacks on sovereign states.[12] Countries across the world have recognized that the benefits of cybersecurity are not mutually exclusive to one sector.[13] Some have gone so far as to suggest that a successful cyber defense collaboration requires cooperation between the public sector, private sector, military, and

---

7. Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, N.Y. TIMES (Feb. 5, 2015), *available at* https://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html (last visited Apr. 10, 2018).

8. *Cyberattacks on the Rise: Are Private Companies Doing Enough to Protect Themselves?*, PWC: GROWING YOUR BUS., 1, *available at* https://www.pwc.com/us/en/private-company-services/publications/assets/pwc-gyb-cybersecurity.pdf (last visited Apr. 10, 2018).

9. *Id.*

10. *Why do Hackers Want to Attack Small Businesses?*, NAT'L CYBERSECURITY INST. AT EXCELSIOR COLLEGE: CYBER EXPERTS BLOG (Feb. 10, 2016), *available at* http://www.nationalcybersecurityinstitute.org/general-public-interests/why-do-hackers-want-to-attack-small-businesses/ (last visited Apr. 10, 2018).

11. Kim Zetter, *We're at Cyberwar: A Global Guide to Nation-State Digital Attacks*, WIRED (Sept. 1, 2015), *available at* https://www.wired.com/2015/09/cyberwar-global-guide-nation-state-digital-attacks/ (last visited Apr. 10, 2018).

12. Daniel B. Garrie & David N. Lawrence, *The Need for Private-Public Partnerships Against Cyber Threats — Why A Good Offense May Be Our Best Defense.*, THE HUFFINGTON POST (Jan. 1, 2016), *available at* http://www.huffingtonpost.com/daniel-garrie/the-soft-power-war-isis-d_b_8818866.html (last visited Mar. 28, 2018).

13. Sean D. Carberry, *The Challenge of Liability Protection for Cyberthreat Sharing*, FCW (Sept. 27, 2016), *available at* https://fcw.com/articles/2016/09/27/cyber-liability-carberry.aspx (last visited Mar. 22, 2018); G.A. Res. 71/28, pmbl., ¶ 5 (Dec. 5, 2016).

citizens of each nation.[14] While the PPP concept has experienced significant growth – over half of all countries report relationships between the public and private sectors[15] – there is still significant room for improvement on the international plane if cyberattacks are to be effectively countered. To bridge this gap, private entities and governments must break the mold and willingly collaborate with one another across sectors.[16]

A. Purpose and Importance of Partnerships

PPPs are hardly a concept unique to cybersecurity.[17] However, the goal of establishing effective relationships between public and private sectors specific to cybersecurity, is to facilitate the exchange and sharing of information regarding cyber threats, common trends in attacks, prevention of attacks, and action in certain instances.[18] The need for partnerships is recognized within individual nations across the world as well as by the international community. The U.N. General Assembly recognized the need for countries to "[p]romote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures."[19]

In addition to clear-cut criteria regulating the partnerships, the most effective partnerships are founded "on trust, clear legal guidance, a bottom-up approach for efficient operation, and community involvement . . . for the betterment of society."[20] Though all of the elements contribute to an effective partnership, the most essential element for both sectors is trust, which necessarily takes time to establish.[21] However, in a climate

14. *See* Grobler et al., *supra* note 1, at 39 (using South Africa as an example).

15. United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, at xxvii (Draft Feb. 2013), *available at* https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last visited Mar. 21, 2018) [hereinafter UNODC].

16. EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES 19 (2013).

17. Madeline Carr, *Public–private partnerships in national cyber-security strategies*, 48, *available at* https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf (last visited Apr. 11, 2018).

18. UNODC, *supra* note 15.

19. G.A. Res. 58/199, at 3 (Jan. 30, 2004).

20. Max Manly, *Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership*, 8 J. OF STRATEGIC SEC. 85, 85 (2015).

21. *Id.* at 90.

where cyberattacks are frequent and evolving, this paradox does not assist timely defense efforts.

B. Obstacles to Successful Collaborations

1. Lack of Transparency

Possibly the biggest concern surrounding PPPs is the lack of trust that inherently exists between the two sectors. Although part of this notion will be discussed in detail below,[22] it is worth noting as an overarching concept that the partnership "will never be completely transparent."[23]

This concept may require more effort from the public sector than from the private sector. Under the National Cybersecurity and Communications Integration Center (NCCIC) model, private sector representatives are granted security clearance to join government representatives in a secure environment where both parties can view classified information and work directly with each other.[24] By inviting private sector representatives into government facilities, the public sector is attempting to instill confidence in the private sector.[25] However, this level of trust cannot be established in one instance or even prior to the actual implementation of the partnership. Rather, both sectors must be responsible for having an initial level of trust for the other so the partnership has a better chance of succeeding from the start.

2. Governmental Regulation of the Private Sector

Before one can consider a partnership between the public and private sectors, governmental overregulation is a concern that must be addressed.[26] A vast majority of private entities are reluctant to have their cybersecurity departments regulated by the government for a multitude of reasons. First, corporations and other private entities want to

---

22. *See infra* section III.B.d.

23. Manley, *supra* note 20, at 91.

24. *See* Rachel Nyswander Thomas, *Securing Cyberspace Through Public-Private Partnership: A Comparative Analysis of Partnership Models*, CTR. FOR STRATEGIC & INT'L STUD. 1, 21 (2012), *available at* https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130819_tech_summary.pdf (last visited Apr. 11, 2018).

25. *Id.*

26. *See* Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, INST. FOR COMMUNITARIAN POL'Y STUD., GEO. WASH. U. (Dec. 19, 2014), *available at* https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity (last visited Apr. 11, 2018).

autonomously decide what works best for their companies.[27] Privately-run corporations are hesitant to follow government-imposed regulations that would facilitate a partnership due to fear of loss of autonomy.[28] To ensure the private sector does not feel it is being overregulated by governmentally-imposed regulations, there needs to exist some level of trust that the government will not interfere with corporate activities beyond what is necessary to prevent and defend against cybercrime.[29]

As this process is one which requires significant resources, private entities fear that governmental regulation will come along with substantial costs that would render corporations "incapable of meeting profitability."[30]

Private entities fear that overregulation from the government will hinder corporate innovation, flexibility, and creativity.[31] Part of this worry comes from the notion that the government's oversight of a corporation's activities regarding cybersecurity information could provide information about the entity that might be used against them in a subsequent legal or regulatory action.[32] A partnership cannot be unilateral. Each sector must provide and accept input and advice from the other in order for there to be an effective, working relationship between the two sectors.[33]

An approach to partnerships that focuses on working from the bottom up may be the most effective way to prevent the private sector from feeling dictated and micro-managed by a governmental entity.[34] Australia, for example, forces corporations to participate in cybersecurity

27. *Id.*

28. *See* Ronald D. Lee & Nicholas L. Townsend, *New Government Cybersecurity Standards Could Impact Many Companies*, LEXOLOGY (Aug. 12, 2013), *available at* http://www.lexology.com/library/detail.aspx?g=d5650eac-65dd-42de-8784-5c62f5798b94 (last visited Apr. 11, 2018).

29. Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, THE CTR. ON L. AND SEC., N.Y.U. SCHOOL OF LAW 1, 3 (2004), *available at* www.lawandsecurity.org/wp-content/uploads/2016/. . /Cybersecurity.Partnerships-1.pdf (last visited Apr. 11, 2018).

30. Etzioni, *supra* note 26.

31. Amitai Etzioni, *Cybersecurity in the Private Sector,* ISSUES IN SCI. AND TECH., *available at* http://issues.org/28-1/etzioni-2/ (last visited Apr. 11, 2018); Etzioni, *supra* note 26.

32. Andrew Nolan, *Cybersecurity and Info. Sharing: Legal Challenges and Solutions*, CON. RESEARCH SERV. 37 (2002), *available at* https://www.fas.org/sgp/crs/intel/R43941.pdf (last visited Apr. 11, 2018).

33. *See* Grobler et al., *supra* note 1, at 34.

34. Manly, *supra* note 20.

defense and to share internal data regarding attacks.[35] Corporations that are regulated without choice are more likely to feel overregulated by the government and less likely to want to share important information.[36]

3. Exposition of Hacks Could Hinder Economic Growth and Hurt Their Public Image

The private sector is reluctant to participate in open information sharing with governmental bodies because doing so might lead the public to believe that companies are economically weak or insecure.[37] Larry Clinton, of the Internet Security Alliance, categorized the plan of information sharing between the two sectors as counterintuitive by requiring private businesses to disclose their security statuses to the public.[38]

However, the more private corporations are encouraged to disclose their breaches, the more succeeding victims will be willing to follow suit. Google's announcement in 2009 of a security breach allegedly perpetrated by China is an example of this "if it happened to Google, it could happen to anyone" mindset.[39] The reluctance to announce cybersecurity breaches in fear of harming the corporation's public image could be eliminated if more corporations were open and candid about their susceptibility to outside attacks.

Some companies also claim that the very existence of a partnership with the government could hinder their public image.[40] This fear can only be removed by a solid, well-established partnership between the two sectors.[41] It will be difficult for companies' customers and investors to

35. Corey P. Gray, *Cyber Utilities Infrastructure and Government Contracting*, UNIV. OF MIAMI NATL. SEC. & ARMED CONFLICT L. REV. 151, 162 (2013); *see also* Manly, *supra* note 20.

36. *See generally* Manly, *supra* note 20.

37. *See* JUDITH H. GERMANO, CYBERSECURITY PARTNERSHIPS: A NEW ERA OF PUBLIC-PRIVATE COLLABORATION (NYU School of Law, Center on Law and Security 2014), *available at* http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf (last visited Mar. 21, 2018).

38. *See* ISSUES IN SCI. AND TECH., *supra* note 31 (explaining that corporations may be "shamed" if breaches are discovered and publicly disclosed).

39. Shane Harris, *Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State*, SALON (Nov. 16, 2014), *available at* https://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/ (last visited Apr. 11, 2018).

40. *See* Manly, *supra* note 20, at 97. "The reluctance to join in a PPP could likely be credited to the potential for the government to gather mass amounts of sensitive information on company and customer information . . . ." *Id.*

41. *See id.*

place their trust in a corporation that does not trust its own data-sharing relationship with the public sector.

4. Disclosure of Confidential Information to the Opposite Sector

Each sector has a justified concern in protecting its own confidential information, even in the midst of sharing information to counter a threat as important as foreign cyberattacks. Governments naturally do not want confidential, protected information leaked to the general public or to private entities. In 2011, the U.S. White House Office of the Press Secretary issued a Cybersecurity Legislative Proposal which recognized the need for protection of government cyber-equipment and networks.[42]

The private sector holds a well-founded concern that the potential disclosure of internal business information might be used for unauthorized purposes by the government or by its business competitors.[43] Some method of removal and protection of this confidential information from the outset of a partnership needs to be negotiated and established prior to information sharing between the two sectors.[44]

5. Lack of Confidence in Public Sector's Ability to Regulate Themselves

It is difficult for the private sector to fully put its faith in the public sector when the public sector is so susceptible to cyberattacks itself.[45] In 2015, Canadian governmental agency servers were attacked likely by "[hostile] foreign governments."[46] France was victim to 24,000 cyber-

42. *See generally* Press Release, White House Office of the Press Secretary, Fact Sheet: Cybersecurity Legislative Proposal (May 12, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal (last visited Mar. 21, 2018).

43. *See* EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R42409, CYBERSECURITY: SELECTED LEGAL ISSUES (2013).

44. *See* Eric O'Neill, *Government's Efforts to Raise the Standard for Cyber Security with New Threat Sharing Regulation Still Problematic*, THE HILL (June 17, 2016), *available at* http://thehill.com/blogs/congress-blog/technology/283914-governments-efforts-to-raise-the-standard-for-cyber-security (last visited Mar. 29, 2018).

45. *See* Jody Westby, *The Government Shouldn't Be Lecturing Private Sector On Cybersecurity*, FORBES (June 15, 2015), *available at* http://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/#b6bf79c38d64 (last visited Mar. 21, 2018).

46. Ben Makuch, *Canada Discovers It's Under Attack by Dozens of State-Sponsored Hackers*, VICE (Jan. 25, 2016), *available at* https://news.vice.com/article/canada-discovers-its-under-attack-by-dozens-of-state-sponsored-hackers (last visited Mar. 29, 2018); *see also Canadian Government Websites go Dark After 'Cyber Attack,'* BBC (June 17, 2015), *available at* http://www.bbc.com/news/world-us-canada-33170534 (last visited Apr. 17, 2018).

threats[47] and the U.S. Internal Revenue Service was victim to a cyberbreach which disclosed information from an unknown number of taxpayer accounts, however is estimated that between 104,000 and 700,000 accounts were compromised.[48] Attacks on the national infrastructure of foreign states have become increasingly more common in recent years.[49] Cybercrime successfully carried out on foreign governments damages both national "economies and State credibility."[50] As these attacks become more frequent and successful, private entities are less likely to put their trust in governmental bodies.

The private sector would most likely have more faith in trading information and confidential cybersecurity operations with the public sector if the public sector was not victim to cyberattacks on such a frequent basis. Nevertheless, French Defense Minister Jean-Yves Le Drian claimed that in regard to the 24,000 cybersecurity threats that "thousands . . . had been blocked."[51] This suggests that it may be beneficial for private corporations to reconsider their ambivalence towards partnership with the public sector based on the perceived inability of the public sector to defend against cyberattacks.

6. Information Sharing as a One-Way Street

The inevitable confidential nature of any nation's government and its agencies creates worry amongst private entities that sharing will not be reciprocated.[52] To eliminate any potential imbalance of shared information, specific limits should be established at the outset of negotiations between a PPP that clarify exactly what type of information will be shared. It is in the interest of both sectors for these limits to be established prior to the entering into an agreement so that this issue does

47. *France Thwarts 24,000 Cyber-Attacks Against Defence Targets*, BBC (Jan. 8, 2017), *available at* http://www.bbc.com/news/world-europe-38546415 (last visited Feb. 18, 2018).

48. *See* Rick Link, *What you Need to Know About the Cybersecurity Information Sharing Act of 2015*, ISACA (Oct. 10, 2016), *available at* https://www.isaca.org/cyber/cyber-security-articles/Pages/what-you-need-to-know-about-the-cybersecurity-information-sharing-act-of-2015.aspx (last visited Feb. 18, 2018); *see also* Kevin McCoy, *Cyber Hack Got Access to Over 700,000 IRS Accounts*, USA TODAY (Feb. 26, 2016), *available at* http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/ (last visited Feb. 18, 2018).

49. *100% increase in cyber attacks will overwhelm critical infrastructure*, INFORMATION AGE (Dec. 6, 2017), *available at* http://www.information-age.com/increase-cyber-attacks-overwhelm-critical-infrastructure-123469887/ (last visited Apr. 17, 2018).

50. Grobler et al., *supra* note 1, at 35.

51. *France Thwarts 24,000 Cyber-Attacks Against Defence Targets*, *supra* note 47.

52. Germano, *supra* note 29, at 3.

not become an obstacle to real-time information sharing throughout the course of the partnership.

7. Lack of Real-Time Information Sharing

Aside from the list of concerns the private sector may claim as reasons for hesitancy towards engaging in a PPP, it is within the best interests of private entities to consider participation for the sole possibility of reduced legal issues due to reduced cybersecurity breaches.[53] The more private entities become victims to cyberattacks, whether they compromise customer information or not, the more susceptible they are to lawsuits filed by angered customers or clients.[54]

Because of the autonomy they enjoy, private companies typically have the technology and means to expediently respond to cyberattacks. However, due to "bureaucratic and other constraints," the government does not enjoy the same amount of flexibility that the private sector does in this regard.[55] Depending on the structure of the partnership, if the government is the sector that happens to be leading a specific cyberattack investigation, the private company victim to the attack might miss out on valuable time that they could be responding to the threat with their own expedient methods and resources.[56]

Some suggest that the only way to effectively approach real-time information sharing between the public and private sectors might be an untraditional one.[57] Because cyberattacks are a relatively recent form of warfare, those who aim to effectively counter these attacks might be forced to abandon their traditional views on cooperation between the public and private sectors.[58]

C. Existing Collaborations: What We Can Learn and What We Can Fix

Learning from past and current failures and triumphs in the cyber world will help create a more effective defense system in the future. In order to craft an ideal U.N. organization that oversees cyber defense,

---

53. Markus Rauschecker, *Thinking Ahead – Implementing the NIST Cybersecurity Framework to Protect from Potential Legal Liability*, U.S. CYBERSECURITY MAG., 35, *available at* https://www.mdchhs.com/wp-content/uploads/UM-CHHS_article_USCYSU14.pdf (last visited Apr. 11, 2018).

54. *Id.* at 36.

55. Germano, *supra* note 29, at 3.

56. *Id.* at 11.

57. TUNNE KELAM, *Cyber Space-Ultimate Case for Trust,* THE EUROPEAN FILES: CYBERCRIME, CYBERSECURITY, AND CYBERDEFENCE IN EUROPE 14 (2016).

58. *See id.*

PPPs, and international cohesion, existing collaborations should be examined so issues can be eliminated from the outset. Taking a preliminary, proactive, and comprehensive look at issues surrounding existing partnerships will have a positive impact on eliminating these potential problems, and will ideally set up for a more functional overseeing body.

1. Overseeing Bodies

In the U.S., the Cyber Command specifically oversees the operations of the Department of Defense networks, while the Department of Homeland Security defends all other U.S. government networks.[59] Both the United Kingdom (U.K.) and Canada employ a central body to oversee national cybersecurity, while "Estonia, France, the Netherlands, and NATO have departments . . . specifically for cybersecurity."[60] Both the Danish Security and Intelligence Service and the European Union's (E.U.) approaches are slightly different from those nations that employ a centralized focus in that they assign departments responsibilities over different sectors.[61]

Some suggest that approaches similar to those instituted by Denmark and the E.U. require significant coordination in order to be successful.[62] Systems that are not coordinated by one governing cybersecurity body pose potential instability issues, as well as inconsistent communication between branches.[63] International cybersecurity efforts can only be as strong as the weakest nation's efforts,[64] therefore suggesting that more consistent domestic approaches would only benefit international coordination.

Though international cooperation is implicated by the fact that the governing bodies of cybersecurity vary tremendously across nations, it is beneficial to consider the array of different approaches nations take. Evaluation of the methods used by different countries allows international efforts to be more comprehensively developed, especially by a governing body such as the U.N. Some have suggested going so far as mapping out all governing cyber institutions as a first step towards

59. Neil Robinson, *Cybersecurity Strategies Raise Hopes of International Cooperation*, RAND CORP., *available at* http://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cybersecurity-strategies-raise-hopes-of-international-cooperation.html (last visited Mar. 19, 2018).

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. Robinson, *supra* note 59.

"seamless cooperation" between nations to counter cybersecurity.[65] With seamless cooperation as the goal, it is with this interest in mind that all cooperating nations should be willing to contribute their most effective and ineffective approaches towards cybersecurity.

One proposed method of an integrated overseeing body between the public and private sectors was set forth by the U.S. Intelligence and National Security Alliance (INSA) Cyber Task Force, suggesting that an "executive committee" should be established, consisting of both corporate executives and governmental officials.[66] The INSA Cyber Task Force emphasized the government's role as superior in such a partnership, as only the government has the "legitimacy to regulate industry where private citizens' interests are at risk."[67] While this notion may be partially true, full or even majority governmental control over a PPP would not be beneficial for an effective defense system against cyberattacks. The private sector will inevitably feel inferior, opening up the possibility of hindered cooperation between branches.

In order for cybercrime to be effectively countered on an international level, it is in every state's best interest that foreign approaches are considered, evaluated, mended if needed, and eventually harmonized. There is a higher chance of success at diminishing foreign cybercrime if there is a more cohesive, universal approach to the issue rather than various uncoordinated efforts emanating from different countries around the world.

2. Current and Operating Collaborations

Many nations currently have cybersecurity PPPs in place. Examining the domestic partnerships that other nations have is beneficial to the creation of an overseeing U.N. body so effective collaborations can be replicated, and troublesome collaborations can either be fixed or avoided.

The European Commissioner for Digital Economy and Society planned to "establish a contractual public-private partnership on cybersecurity" in 2016 that required participation from a range of actors including national security agencies, to cyber-equipment producers, to

65. *Id.*

66. *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models, Intelligence and National Security Alliance* 1, 3 (2009), *available at* https://www.insaonline.org/wp-content/uploads/2017/04/INSA_AddressingCyber_WP.pdf (last visited Mar. 22, 2018) [hereinafter INSA].

67. *Id.*

critical infrastructure operators.[68] The European Cybersecurity Strategy launched a program that integrates the public and private sectors and addresses research priorities, identifies common and prevalent issues, and discusses common outcomes of cybersecurity efforts.[69] The strategy also looks into ways in which both sectors can focus and organize research efforts.[70] Portugal in particular has recognized the importance of information sharing between the public and private sectors with the common goal of eventually regulating cybersecurity on the global level.[71]

In the U.S., the Federal Bureau of Investigation (FBI) has recently become more involved in engaging with the private sector to participate in public awareness efforts.[72] One of the more well-known alliances between the U.S. government and a private entity is that between the National Security Agency (NSA) and Google. After Google was the victim of a large-scale cyberattack in 2009, it was announced in The Washington Post that Google had partnered with the NSA with the main goal of proactively defending Google from future cyberattacks.[73] Neither organization officially commented on their alleged partnership.[74] Allegedly, however, information was shared between the two groups, though Google did not share "proprietary data" with the NSA while the NSA did not have access to Google users' searches or email accounts.[75] According to sources connected to the alliance, Google agreed to provide

---

68. Gunther H. Oettinger, *Partnerships to step up cybersecurity in Europe*, THE EUR. FILES: CYBERCRIME, CYBERSECURITY, AND CYBERDEFENCE IN EUR., Jan. 2016, at 6, 7.

69. *See Public Private Partnership on Cybersecurity*, EUR. COMM'N (Dec. 14, 2015), *available at* ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf (last visited Apr. 17, 2018).

70. *See id.*

71. *See* U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 17-18, U.N. Doc. A/71/172 (July 19, 2016).

72. *Statement Before the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence*, FBI (June 28, 2012), *available at* https://archives.fbi.gov/archives/news/testimony/economic-espionage-a-foreign-intelligence-threat-to-americans-jobs-and-homeland-security (last visited Mar. 26, 2018); Melanie Reid, *A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?*, 70 U. MIAMI L. REV. 757, 767 (2016).

73. Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, WASH. POST, (Feb. 4, 2010), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html (last visited Mar. 26, 2018); Stephanie A. DeVos, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J., 172, 200-01 (2011); *see also* Harris, *supra* note 39.

74. Nakashima, *supra* note 73.

75. Nakashima, *supra* note 73; DeVos, *supra* note 73, at 201.

traffic information on its networks in exchange for information on foreign hackers from the NSA.[76]

Direct partnerships similar to that between the NSA and Google are virtually impossible to establish on a national, never mind global, scale due to the sheer volume of governmental agencies and private corporations that exist. However, such partnerships are ideal in that they can be mutually beneficial in that parties to this type of relationship could possibly offer information to the other party in exchange for reciprocal information or protection.[77] It is widely accepted that the public sector has adequate resources and ability to defend against cyberattacks.[78]

In 2013, the U.S. government (specifically the National Institute of Standards and Technology within the Department of Commerce) implemented a program called the Cybersecurity Framework as the result of collaboration between the government and private sector.[79] This framework uses commonplace language to suggest methods of cybersecurity management that private entities can follow, without making such methods mandatory.[80] While this framework is not binding on corporations, ideally they would see the benefits that this program (or one similar implemented in countries outside of the U.S.) provides and would eventually adopt a similar program on their own accord.

Also in the U.S. is the NCCIC, a 24-hour center which shares cybersecurity information across both government entities and the private sector.[81] This model appears extremely beneficial for the real-time information sharing portion of PPPs as well as confidence-building between the two sectors. Nevertheless, it is important to consider where the government should draw the line in term of granting the private sector access to the center. Should a line be drawn, or should the government maintain an "all are welcome" attitude so as to include as many corporations as possible? These threshold issues are among those which

---

76. Harris, *supra* note 39.

77. *Id.*

78. Germano, *supra* note 29, at 2.

79. Rauschecker, *supra* note 53, at 35-36.

80. *See id.*

81. *About the National Cybersecurity and Communications Integration Center (NCCIC)*, HOMELAND SEC., (June 22, 2017), *available at* http://www.dhs.gov/xabout/structure/gc_1306334251555.shtm (last visited Mar. 26, 2018); *see also* RACHEL NYSWANDER THOMAS, SECURING CYBERSPACE THROUGH PUBLIC-PRIVATE PARTNERSHIP: A COMPARATIVE ANALYSIS OF PARTNERSHIP MODELS 19 (2012), *available at* https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130819_tech_summary.pdf (last visited Apr. 17, 2018).

can be incorporated and negotiated by an organ of the U.N. in setting forth guidelines for PPPs.

While many European nations have strong national cybersecurity strategies in place, as of 2015 the majority have not formalized or implemented a PPP, and rather have informal relationships between the public and private sectors.[82] France's cybersecurity strategy, the French National Digital Security Strategy, recognizes the importance of PPPs,[83] however France has not formally established any such program.[84]

Germany has an exceptionally strong PPP system in place known as UP KRITIS.[85] UP KRITIS defines the goals of the initiative specific to each department involved, recognizing that the goals of every single governmental and private sector are not going to be exactly the same.[86] The German government first recognized the need for a partnership with the private sector in 2005.[87] Through UP KRITIS, concepts from both sectors are compiled together and eventually implemented, training exercises are held, and a system for "crisis management" is established.[88] UP KRITIS emphasizes a network of trust between all members, specifically during the exchange of confidential information.[89] Because trust is such an essential element to a successful partnership between the two sectors, the U.N. should follow UP KRITIS's emphasis on establishing trust from the outset of collaborations. Knowing that trust is an issue for each sector is an important first step to build on, as this can be a platform upon which the U.N. operates to create this environment from the start.

As the risk to cybersecurity and attacks inevitably evolves, some call on the public sector to proactively predict the evolution of these sophisticated threats, and have both safeguards and countermeasures in

---

82. *See* BSA, EU CYBERSECURITY DASHBOARD, A PATH TO A SECURE EUROPEAN CYBERSPACE 11-16 (2015).

83. GEN. SECRETARIAT FOR DEF. NAT'L SECURITY, FRENCH NAT'L DIGITAL SEC. STRATEGY 3 (2015), *available at* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (last visited Mar. 26, 2018).

84. *See id.*; CYBERSECURITY DASHBOARD, *supra* note 84, at 13.

85. *See* UP KRITIS, FED. OFF. INFO. SEC., UP KRITIS: PUBLIC-PRIVATE PARTNERSHIP FOR CRITICAL INFRASTRUCTURE PROTECTION (2014), *available at* http://www.kritis.bund.de/SubSites/Kritis/EN/publications/Fortschreibungsdokument_engl..html (last visited Mar. 26, 2018).

86. *See id.*

87. *Id.* at 29.

88. *Id.* at 7.

89. *Id.* at 29.

place to evolve along with the attacks.[90] The focus of establishing cooperative and effective partnerships between the private and public sectors should be on determining how each sector's contributions can fit together in order to best counter the attacks.[91]

As one of the leading investigative bodies in the U.S., the FBI's longstanding recognition and appreciation of the private sector's willingness to work with the public sector[92] is an essential step towards an effective partnership. Further, the U.S. approach to insulating liability for the private sector is one that would only be beneficial if practiced by all countries, with the end goal of integrating both the public and private sectors. The U.S. proposes that liability protection should be offered to protect the private entities from losing profits as a byproduct of sharing information with the public sector.[93] Establishing private sector trust in the federal government is crucial to the success of information sharing between the two sectors. In establishing what some call a "reverse Miranda protection," essentially nothing the private sector shares with the government can be used to against it.[94] Penny Pritzker, U.S. Commerce Secretary, emphasized at the Chamber of Commerce Cybersecurity Summit that failure to foster the private sector's trust in the public sector would not only leave the country vulnerable to outside cyberattacks, but would "risk slowing the pace of American innovation."[95] Governments hoping to establish successful and seamless partnerships between the public and private sectors need to recognize this concept of allowing the private sector to retain a certain level of autonomy. The risk in removing any of the freedoms the private sector would normally retain if it were not for the partnership with the public sector threatens to interfere with internal economies on a much larger scale.

---

90. Danilo D'Elia, *Public-Private Partnership: The Missing Factor in the Resilience Equation - The French Experience on CIIP*, THE CIP REP., 13 (Feb. 2015), *available at* http://www.cyberstrategie.org/sites/default/files/media/danilo_delia_extrakt_-_public-private_partnernship_the_missing_factor_in_the_resilience_equation_the_french_experience_on_ciip_.pdf (last visited Mar. 26, 2018).

91. *Id.*

92. Thomas T. Kubic, *Before the House Committee on the Judiciary, Subcommittee on Crime*, FBI, (June 12, 2001), *available at* https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem (last visited Mar. 26, 2016).

93. Etzioni, *supra* note 26.

94. Sean D. Carberry, *The Challenge of Liability Protection for Cyberthreat Sharing*, FCW (Sept. 27, 2016), *available at* https://fcw.com/articles/2016/09/27/cyber-liability-carberry.aspx (last visited Apr. 3, 2018).

95. *Id.*

3. Benefits to the Private Sector

While both the public and private sectors have many justifiable concerns regarding partnership, the most effective way to overcome these concerns would be to address them from the start of negotiations. This would ensure that potential issues do not arise unexpectedly, undermining the mutually beneficial aspects that the partnership creates.

As cybersecurity evolves and expands, the notion of consistency, especially among the private sector, may become more important from a legal perspective. Courts that are faced with cybersecurity breach lawsuits may look for one standard to hold the private entities accountable.[96] With multiple varying pieces of legislation, standards of care, and frameworks in place that quasi-govern the private sector's regulation of cybersecurity, it is difficult to hold these private entities to the same, even level of care.

IV. INTERNATIONAL EFFORTS: LEGISLATION, COOPERATION, AND ISSUES

Many countries rely heavily on international law both to encourage active participation in international information sharing and to help establish and encourage partnerships between the public and private sectors.

A. International Law Governing Collaboration and Cooperation Between Nations

The need for international cooperation and some level of information sharing across nations stems from the idea that one nation alone does not hold all of the resources necessary to defend against cyberattacks.[97] One example of an exemplary system of international information sharing is the "Five Eyes" – the U.S., Canada, New Zealand, Australia, and the U.K.[98] While the specifics of this alliance are not publicly known, these five countries operate under the general premise of sharing top-secret cyber intelligence.[99] One nation alone cannot target and

96. Rauschecker, *supra* note 53, at 36.

97. *See* Alexander Moens et al., *Cybersecurity Challenges for Canada and the United States*, FRASER INST. (Mar. 2015) 21, *available at* https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf. (last visited Apr. 3, 2018).

98. *Id.* at 20.

99. *See Privacy International Launches International Campaign for Greater Transparency Around Secretive Intelligence Sharing Activities Between Governments*, PRIVACY INT'L (Oct. 13, 2017), *available at* https://www.privacyinternational.org/node/51 (last visited Apr. 3, 2018).

effectively counter every cyberattack that is mounted against it.[100] Keeping pace with evolving threats and funding research that goes into the defense against cyberattacks are both tasks that are achieved with higher success with cooperation amongst nations.[101]

Individual nations have enacted policies to encourage international cooperation in cybercrime defense. South Africa, for example, drafted a cybersecurity policy that set forth the framework for encouraging international cooperation and compliance with existing cybersecurity standards.[102] These are the types of policies or ideologies that nations should adopt in order to promote international cooperation in cybersecurity.

There are a range of agreements addressing cybersecurity that currently govern, dictate, and suggest methods of international cooperation. Bilateral and multilateral treaties between nations have become more prevalent, fostering agreements to work together and share intelligence regarding threats and attacks. In 2007, Turkey, the U.K., and Northern Ireland agreed to cooperate within their own capacities to assist in the prevention, detection, and suppression of cybercrimes.[103] China and France entered into a similar agreement in 2008, agreeing to assist each other in combatting cybercrime.[104]

While bilateral and multilateral treaties may be effective for the nations they are between, these agreements are not as effective on a global level in uniting as many nations as possible to work together with the goal of successfully countering cyberattacks. The more forceful, binding, and, eventually effective method for international cooperation might be one that is employed on a much larger scale and by one overseeing body. In 2001, the Council of Europe established common goals between European states and other signatory parties at the Budapest Convention on Cybercrime.[105] The Convention recognized the need for cooperation between states' public and private sectors, as well as international

100. *See* Moens et al., *supra* note 97, at 21.

101. *See id.* at 23.

102. Grobler et al., *supra* note 1, at 35.

103. Memorandum of Understanding between the Government of the Republic of Turkey and the Government of the United Kingdom of Great Britain and Northern Ireland on cooperation in combating terrorism, serious crime and organised crime. (Mar. 12, 2007), 2503 U.N.T.S. 44746.

104. *See* Agreement on cooperation in the field of internal security between the Government of the French Republic and the Government of the People's Republic of China art. 2, Sept. 10, 2006, 2515 U.N.T.S. 44911.

105. *See* Convention on Cybercrime, pmbl., Nov. 23, 2001, E.T.S. 185.

cooperation in prosecuting cybercrime.[106] Similarly, the U.N. General Assembly has recognized "the importance of international cooperation for achieving Cybersecurity."[107] The governance of the U.N. over international cybersecurity cooperation would provide a large amount of organization over the collaborations, which would eventually lead to a more cohesive system of information sharing between cooperating nations.

In addition to the Budapest Convention, 41 countries are members of the Wassenaar Arrangement[108] (Arrangement), which is a platform that has been established to contribute to international security by keeping "intrusion software," *inter alia*, out of the hands of terrorists.[109] The Arrangement is voluntary[110] and it is the responsibility of the nations' legislators to incorporate the regulations, as set forth in the Arrangement, into their respective legislation.[111] This type of arrangement is ideal in nature: it incorporates, and thus quasi-regulates, a large number of leading nations (including the U.S., the U.K., Russia, Canada, and Australia[112]), and sets forth consistent international security guidelines for nations to follow.[113]

However, this specific Arrangement has been victim to significant criticism over the past couple of years. The Coalition for Responsible Cybersecurity (CRC), an organization formed to prevent the U.S. government from adopting certain regulations that could negatively impact U.S. cybersecurity efforts,[114] agrees with the general principles of Wassenaar, however considers the Arrangement to be "overly broad."[115]

---

106. *Id.*

107. G.A. Res. 58/199, at 2; U.N. Doc. A/RES/58/199 (Jan. 30, 2004).

108. Bill Camarda, *'Meltdown' over international cybersecurity agreement*, NAKED SEC. BY SOPHOS, *available at* https://nakedsecurity.sophos.com/2016/12/28/meltdown-over-international-cybersecurity-agreement/ (last visited Apr. 19, 2018).

109. The Wassenaar Arrangement, *available at* http://www.wassenaar.org/ (last visited Apr. 4, 2018); Camarda, *supra* note 1.

110. Tami Abdollah, *US fails to renegotiate arms control rule for hacking tools*, ASSOC'D. PRESS (Dec. 19, 2016), *available at* http://bigstory.ap.org/article/c0e437b2e24c4b68bb7063f03ce892b5/us-fails-renegotiate-arms-control-rule-hacking-tools (last visited Apr. 19, 2018).

111. Camarda, *supra* note 108.

112. *Id.*

113. *See* The Wassenaar Agreement, *supra* note 109.

114. About Us, COALITION FOR RESPONSIBLE CYBERSECURITY, *available at* http://www.responsiblecybersecurity.org/aboutus/ (last visited Feb. 12, 2018).

115. Tom Reeve, *Wassenaar Arrangement 'inhibits international cyber-security efforts'*, SC MEDIA UK (July 21, 2016), *available at* https://www.scmagazineuk.com/wassenaar-arrangement-inhibits-international-cyber-security-efforts/article/530845/ (last visited Apr. 19, 2018).

Because Wassenaar's goal is to prevent terrorists from acquiring technological developments in "intrusion software,"[116] its essential consequence is a dichotomy in that it also "impede[s] the ability of the international cyber-security community to respond in a timely manner to threats and attacks."[117] Though it attempts to prevent exactly this, Wassenaar is criticized for having a detrimental effect on cybersecurity rather than a beneficial one. Wassenaar is further criticized for its negative impact on the private sector.[118] It proposes a system of license applications which critics believe would subject private companies to increased cyberattacks as well as damage internal company data.[119] Further evidencing its problematic nature, the Arrangement is difficult to renegotiate due to the "secrecy that surrounds the negotiations and the resulting policies."[120]

Wassenaar is an ideal agreement of which to base a U.N. model for governing PPPs and international cooperation in that it sets forth specific implementations for countries to follow and is not too broad. However, an agreement that mirrors Wassenaar exactly might have limited effectiveness due to the private sector's hesitancy to put itself at risk by following the regulations. Though a lofty task, nations who are currently a part of Wassenaar would benefit from either attempting to renegotiate Wassenaar and craft it into an implementable model for the U.N., or creating a new agreement with the same specific goals that does not suggest methods that would potentially harm the private sector. Some have also suggested building upon the Budapest Convention[121] which would be beneficial as well, if more specificity can be included.

In 2015, over 20 nations agreed to a U.N. Group of Governmental Experts (GGE) report regarding norms of international security, including China, France, Russia, the U.K., and the U.S.[122] Signatories to

---

116. *See* The Wassenaar Agreement, *supra* note 109; Camarda, *supra* note 108.

117. Reeve, *supra* note 115.

118. *See Wassenaar: Cybersecurity and Export Controls, J. Hearing Before the Subcomm. on Info. Tech. of the H. Comm. on Oversight and Gov't Reform and the Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Tech. of the H. Comm. on Homeland Sec.*, 114th Cong. 66-73 (2016) (written testimony of Dean C. Garfield, President and CEO, Information Technology Industry Council).

119. *Id.* at 68-69.

120. Reeve, *supra* note 115.

121. *Cybersecurity: A global issue demanding a global approach*, U.N. DEP'T OF ECON. AND SOC. AFF., *available at* http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html (last visited Feb. 18, 2018).

122. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, GA Res. A/70/174, July 22,

this report agreed to a level of "cyber diplomacy,"[123] and are called upon to both refrain from engaging in cyberattacks, as well as to protect their own systems to the best of their abilities from foreign attacks.[124] The report goes one step further and warns states against using proxies to carry out such activities.[125] Measures such as the norms set forth in the GGE report can be considered "confidence-building measures" between nations.[126] Cooperation and collaboration within the international community are concepts that both rely heavily upon trust. At the very least, the international community would benefit from some sort of framework that regulates how nations should behave in the cybersecurity realm.[127]

The benefits to establishing an international community, which shares information and takes proactive measures to prevent against cyberattacks, are international peace and security.[128] While this concept is easier said than done, taking a look at the multitude of reports, treaties, and other international agreements that are currently being implemented, and extracting the benefits from each to add to an existing or to create a new governing agreement is in every nations' best interest in cybersecurity defense.

B. Existing International Efforts to Harmonize Public and Private Sectors

Aside from treaties and conventions that govern international cybersecurity cooperation, many nations are already members to large-scale international agreements that encourage partnerships between the public and private sectors for defending against cyberattacks.

In 2004, the Council of Europe held a Conference on the Challenge of Cybercrime (Conference) and called for governments to encourage cooperation between state institutions and the private sector.[129] The Convention on Cybercrime has thirty-seven signatories and has been

---

2015; Tim Maurer, *The New Norms: Global Cyber-Security Agreements Face Challenges*, CARNEGIE ENDOWMENT FOR INT'L PEACE, *available at* http://carnegieendowment.org/2016/02/05/new-norms-global-cyber-security-agreements-face-challenges-pub-63031 (last visited Apr. 11, 2018).

123. Maurer, *supra* note 122.

124. Governmental Experts, *supra* note 122.

125. *Id.*

126. *Id.*

127. Daniel M. Gerstein, *Define Acceptable Cyberspace Behavior*, U.S. NEWS, (Sept. 26, 2015), *available at* http://www.usnews.com/opinion/blogs/world-report/2015/09/26/us-china-cybersecurity-pact-highlights-bigger-issues (last visited Apr. 26, 2018).

128. *See generally* Governmental Experts, *supra* note 122.

129. Conference on the Challenge of Cybercrime, COUNCIL OF EUR., 1 (Sept. 15-17, 2004), *available at* www.anticorruption.bg/fileSrc.php?id=657 (last visited Apr. 18, 2018).

ratified by five nations.[130] One of the objectives of the Conference is to include the chief executives of corporations in the fight against cybercrime, and to request participation from nations, the E.U., and international organizations.[131] This model's inclusivity is one which should be replicated. Its incorporation of officials from not only the public and private sectors, but from intergovernmental institutions already sets the foundation for a PPP that is regulated by the U.N. Though partnerships need to be negotiated mainly between the public and private sectors themselves, including the U.N. would help maintain consistency and provide a neutral intermediary between the two sectors.

Some agreements have been established on a smaller scale than the Conference, yet lend just as much, if not more, insight as to how international information sharing between the public and private sectors might best be effectuated. In 2003, the Asia-Pacific Economic Cooperation hosted a Cyber-Security Workshop where members of the Economic Commerce Steering Group (ECSG) agreed to work with the private sector to exchange information, practices, and policies related to cybersecurity issues with the goal of identifying the most effective practices to counter cyberattacks.[132] The ECSG vowed to work with the private sector to strengthen "the intersection of privacy and security" with the eventual goal of promoting proactive security policies and protections, and consequently, information sharing with other entities.[133] Aside from the underlying goal of cooperation between governments and the private sector, the workshop emphasized the distinct roles of government and private entities in building a secure culture in the cyber world.[134] According to the ECSG, private businesses have an obligation to educate both employees and partners about cybersecurity issues while governments have the duty to develop partnerships with the private sector to facilitate information sharing.[135]

While this agreement is very narrow, its approach is one which the U.N. would benefit from adopting. Cybercrime defense is at its strongest when the public and private sectors are harmonized and the best way to facilitate this partnership is through specific and planned efforts that

130. *Id.*

131. *Id.* at 2.

132. APEC Electronic Commerce Steering Group; 8th Meeting, Phuket, Thailand, 4 (Aug. 15-16, 2003), *available at* http://mddb.apec.org/Documents/2003/ECSG/ECSG2/03_ecsg2_summary.doc (last visited Mar. 26, 2018).

133. *Id.* at 7.

134. *Id.* at 1.

135. *Id.* at 6.

emphasize the importance of collaboration between the public and private sectors of each participating state.[136] It would be in the U.N.'s best interest to consider approaches taken by all different sizes of international agreements, workshops, conferences, conventions, and research groups. By considering these plans, successful approaches can be adopted, and proven problematic approaches can be avoided.

C. Issues with International Cooperation

While treaties and other international agreements are essential to defeat foreign cyberattacks, there are many potential issues that must be evaluated and resolved prior to officially engaging in international information sharing. The most obvious and vital of these issues is the reluctance of foreign governments to risk sharing internal security information with other nations.[137] While nations party to a treaty or international agreement to assist each other in combating cybercrimes may be allies on that particular topic, or at one particular point in time, it is uncertain that those nations will remain allies in the future.[138] The reluctance to share sensitive security information with other states is founded in a justified concern of providing foreign state's information critical to national infrastructure. If all information regarding cybersecurity is shared with allied states, what security is retained in the cyber world and in warfare? In establishing an international agreement, nations should consider this potential dilemma in order to avoid future misunderstandings regarding the sharing of information. The best way in which nations can be successful in forming an effective collaboration to combat cybercrime is through early preparation of possible issues.[139]

Another major issue with effectively countering cybercrime on an international level is the difficulty in recruiting some of the major world powers because of their suspected involvement in cyberespionage. Since many countries are commonly-accused offenders of cyberespionage, a conflict of interest exists in deciding whether to include them in the

136. *See id.*

137. *See* Sico van der Meer, *Foreign Policy Responses to International Cyber-attacks: Some Lessons Learned*, CLINGENDAEL NETH. INST. OF INT'L REL. (2015), *available at* https://www.clingendael..org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf (last visited Mar. 25, 2018).

138. *Id.*

139. *See* Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 J. OF CONFLICT AND SEC. L. 187, 196 (2012).

international effort to defend against these attacks.[140] These countries (with the exception of the U.S.) are viewed by many as those who justify intellectual property theft because they believe it creates a "level playing field amongst developed and developing countries."[141] Nations who are victims of these attacks are less likely to want to work with the nations who are commonly accused of facilitating these types of cyberattacks. This is an issue that would best be left for an overseeing U.N. body to mediate and work through because it is not a nation state itself.

D. U.N. as the Best Governing Mechanism

In order to ensure international cooperation is as close to seamless as possible, the largest international governing body in the world is the best organization to oversee such regulation. The countless variations of agreements that currently exist in today's international community are a step in the right direction, because they set out to tackle the problem of foreign cyber defense. However, the issue is that the agreements are not large-scale, uniform, specific, and inclusive enough to have a lasting and effective impact.[142]

International organizations have become notably authoritative actors in the international community.[143] The U.N. Security Council has been considered "the most powerful supranational organ in the world" with significant impact on the nation-state system.[144] Though some doubt or question how much power the U.N. actually holds in the world today,[145] many still consider it to be influential. Using this powerful, international body is the best method through which to oversee and regulate PPPs and

140. *See* Rita Boland, *Countries Collaborate to Counter Cybercrime*, SIGNAL, (Aug. 2008), *available at* http://www.afcea.org/content/?q=countries-collaborate-counter-cybercrime (last visited Apr. 11, 2018).

141. Reid, *supra* note 72, at 822.

142. *See* Murat Dogrul et al., *Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism*, *in* 3D INT'L CONF. ON CYBER CONFLICT 29, 38 (C. Czosseck et al. eds., 2011).

143. *See* Martin Binder & Monika Heupel, *The Legitimacy of the UN Security Council: Evidence from Recent General Assembly Debates*, 59 INT'L STUDIES QUARTERLY 238, 238 (2015).

144. *Id.*

145. *See generally* Nile Gardiner, *The Decline and Fall of the United Nations: Why the U.N. Has Failed and How It Can Be Reformed*, HERITAGE FOUND. (Feb. 7, 2007), *available at* http://www.heritage.org/report/the-decline-and-fall-the-united-nations-why-the-un-has-failed-and-how-it-can-be-reformed (last visited Apr. 18, 2018).

international cooperation because of the influence it has in the international arena.[146]

V. CONCLUSION

The need for PPPs within the cybersecurity world has long been recognized and is more urgent now than ever with cybersecurity's recent surge as a modern-day form of warfare. Defending against cyberattacks on a global level can best be viewed as a two-step process, and is best implemented by the U.N.

Seamless collaboration within nations between respective public and private sectors is where the world needs to start before cybersecurity can be countered on an international level. Nations would inherently become stronger to fight against these foreign actors if their own domestic sectors are as close to being in tandem agreement as they can in regards to how to best share information and work together to prevent against outside attacks.

The next, equally essential step after domestic cooperation between the public and private sectors is cooperation between nations.[147] Cybersecurity becomes much more effective when it is implemented on a global level, with cohesive standards that nations are able to follow. Cybercrime defense would benefit from uniform standards so that all nations are held to the same standard and all are able to cooperate and collaborate under one uniform organization.

Both of these partnership concepts require significant trust. With well thought-out agreements and cooperative efforts from both the private and public sectors as well as nations across the world, an effective level of cybersecurity can be reached.

---

146. *See* Mahmudul Hasam, *International Cyber Security Cooperation*, MODERN DIPL. (Nov. 13, 2016), *available at* https://moderndiplomacy.eu/2016/11/13/international-cyber-security-cooperation/ (last visited Mar. 26, 2018).

147. *See EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*, BSA: THE SOFTWARE ALL., 3 (Jan. 1, 2015), *available at* http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf (last visited Apr. 11, 2018).