Docket No. 160725650-6650-01

Information on Current and Future States of Cybersecurity in the Digital Economy

Request for Information

Input to the Commission on Enhancing National Cybersecurity

Prepared By: Jake Braun and Helena Bentley, via the University of Chicago

Date: September, 2016

1 EXECUTIVE SUMMARY

Cybersecurity is a national security priority and an economic necessity. A sound cybersecurity policy must protect open commerce, promote innovation, and secure our Nation. It must also chart a course for a public-private collaboration to improve our Nation's overall cyber security posture through the widespread adoption of foundational cyber hygiene. Strategically, a sound cyber security policy will have implications for everything from the U.S. economy, to global human rights, to U.S.-China relations. The following discussion highlights a number of key recommendations to drive cybersecurity policy for the coming years.

1. **Cyber Hygiene—** we must encourage better policy-making by embracing cyber hygiene practices, and supporting general cyber awareness at all levels.
2. **Federal Government Technology Transfer—**we must leverage all exiting collaborative tech transfer initiatives to commercialize methods and products that assist in automating the Top 5 Critical Security Controls.
3. **Reconcile Human Rights and Cybersecurity—** we must lobby for public policy that is aware of and actively responsive to human rights abuses associated with interaction with the cyber world.

The United States, especially those who have been around for the last forty years to witness the growth of the connected world, have seen their incomes rise and their quality of life drastically improve. However, there are millions around the world who have only experienced the dark side of the internet—children who have experienced abuse through the internet, migrants who have suffered at the hands of abusive smuggling schemes, and large swathes of society who are oppressed by political regimes.

As it stands, the U.S. has an overwhelming amount of influence over the governance of the internet. Most of the innovation in internet technology happened in the U.S., and the U.S. has a vested interest in retaining control over the system that makes it so much money and gives it so much influence. We as the nation that created the internet and who actively contribute and benefit most from it must take responsibility for reconciling the potential abuses of our systems against vulnerable populations. At home and abroad, it is the United States' duty to lead the way by aligning our national priorities to demonstrate concern for human rights and to combat creative exploitation of physical people in the virtual world.

2 PREFACE

A major portion of the research conducted for this submission was crafted by students of the Fall 2015 *Intersection of Cyber Threats and Human Rights*; a course at the Harris School of Public Policy at the University of Chicago. Under the guidance of Lecturer Jake Braun, the students spent the term digesting literature on cyber threats and discussing cyber-related policy with experts and industry leaders across the private and public sectors in global cybersecurity. The recommendations outlined in this submission are solely those of Jake Braun, Helena Bentley, and the course students—they do not necessarily reflect the views of the contributors' employers or the University of Chicago.

Authors from Harris School of Public Policy, University of Chicago:
Helena Bentley, A.J. Shattuck, Joshua Krauss, Tess Eckstein, Aseal Tineh, Fumi Kojima, Xin Jin, Jordan Ng, Alex Warofka, Gracelyn Jennings-Newhouse.

3 INTRODUCTION

The legacy of our present leadership will be determined by the actions we take now to prepare for the future. Just as the current generation blames our predecessors for irresponsible management of industrial era technology and rampant disregard for regulating energy consumption, our present leaders must be proactive in their approach to cyber issues. We cannot look back and say that we didn't know better, because the cyber innovations of tomorrow are developing all around us. The future of cybercrime will only be as severe as current governance standards allow it to develop unchecked.

Many of the recommendations outlined in this submission, namely the idea of cyber hygiene and tech transfer promotion, are common-sense approaches to broad issues facing the nation. They are valid, important, and necessary steps towards achieving robust cyber policy, and should not be left out of the conversation. The side-effects of the reality created by the interconnectedness of the physical and cyber world, however, relays upon our society a far less considered issue of human rights implications.

The internet as a phenomenon has been instrumental in the development of the world's population in general. It has created many winners in the global economy—be they internet startups, e-commerce vendors and consumers, government organizations, and more—that have been able to innovate in ways never before dreamed. Educated people and those higher up the economic ladder benefit from interconnectivity, and they use that position to gain the edge over others in the population. People at the bottom, however—like children and those at a higher risk of abuse and exploitation—are forced deeper towards the bottom.[1] These individuals suffer immensely at the hands of criminals that manipulate the internet for their own gain, and it's incumbent upon us and the United States government to take action.[2]

What does it say about our priorities as a nation when we are willing to spend billions of dollars on securing federal government systems through the National Protection and Programs Directorate, but we only spend about $100 million on the HSI division that investigates real-world social evils.[3] It has been demonstrated time[4] and time[5] again that innocent people are being abused by a system that we helped to create. We must lead our society forward by taking responsibility for the fact that we made, and benefit from, the internet. Therefore, we need to take ownership of it by helping those who are being hurt by it or as a result of it.

This discussion seeks to address of the most pressing overarching issues related to governance of cybersecurity. In this era where state boundaries, jurisdiction, and regulation of the cyber landscape defy accepted definition, the Unites States needs to prioritize targets and establish scope and depth of roles to confront challenges head on. Successful governance will only be judged by the measure that leaders, policy makers, and civilians alike become proactive and aware.

[1] Mapping the Digital Divide, Council of Economic Advisers Issue Brief July 2015: https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf

[2] See "Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call", A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf

[3] Fiscal Year 2016 DHS Budget in Brief; https://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf

[4] "Prior to the creation of the agency in 2003, legacy U.S. Customs special agents investigated the disbursement of illegal child pornography that was often sent by mail or purchased overseas. With the advent of the Internet, the sharing and trading of child pornography now primarily occurs online. In addition to the legacy expertise, HSI special agents also have the authority to investigate the illegal movement of people and goods across U.S. borders, and because the Internet is borderless, the sharing of contraband online is an international crime." Child Exploitation Investigations Unit, U.S. Immigration and Customs Enforcement. https://www.ice.gov/predator#wcm-survey-target-id

[5] "New Digital Technologies Produce Unprecedented Levels of Child Abuse Material Online." United Nations Human Rights, Office of the High Commissioner. http://www.ohchr.org/EN/NewsEvents/Pages/Childsexualexploitationonlineontherise.aspx

If we as a society get governance right, we will be adequately prepared to meet the more destructive aspects of future-cybercrime and technological innovation. The components of a successful future-cyber policy include over-arching advocacy and awareness programs to improve cyber hygiene, greater commitment to funding partnerships at every level of government, and strategic planning in research and development of future tech—with an eye towards federal tech-transfer programs to marry our creative innovation with the most reliable funding. What will naturally evolve out of preparedness is a more capable, resilient government and private sector in dealing with the challenges arising from the next frontier of in cybercrime.

4 FUTURE TRENDS

Without question, the next-frontier in cybercrime and cyber warfare will be fought in the Internet of Things (IoT), with defining events over the next decade focusing around the evolving landscape of bring-your-own-device (BYOD) security and point of service (POS) mobile nodes. The United States has already seen the beginnings of this movement away from traditional targets towards personal devices and oft-neglected static infrastructure.[6] These events continue to occur because most consumer products and infrastructure installations are connected in some way through ill-protected networks—be that Z-wave automation[7], radio frequency ID (RFID) and near field communication (NFC) [8], Bluetooth technology[9], or air-gapped LAN systems[10].

As independent security concerns, managing the interconnectedness of our devices will be difficult. When combined with insufficient regulatory policy and funding, brain-drain to the private sector, and increasing availability of hacking products and services available online—the future becomes dangerous. At present, the majority of sophisticated hacking comes from money-rich state-sponsored initiatives, that are minimally guided by a regulating authority for the purpose of some cause.[11] In the future, however, due to free-market forces we may begin to see multi-layer infiltrations by asymmetrical forces—with more sinister agendas.

[6] Verison 2016 Data Breach Investigations Report: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[7] Z-wave comprehensive list of products: http://www.z-wave.com/products

[8] Hacking RFID Tags is easier than you think; Black Hat: http://www.eweek.com/security/hacking-rfid-tags-is-easier-than-you-think-black-hat

[9] Guide to Bluetooth Security, National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf

[10] Air-Gapping SCADA systems won't help you, says man who knows, The Register: http://www.theregister.co.uk/2016/06/03/airgaps_scada_systems_wont_prevent_attacks/

[11] Pawlak, Patryk and Petkova, Gergana. State-Sponsored Hackers: Hybrid Armies? *European Union Institute for Security Studies*: http://www.iss.europa.eu/uploads/media/Alert_5_cyber___hacktors_.pdf

With the introduction of next-generation malware capable of affecting critical physical infrastructure, the nation is becoming increasingly aware of the human implications of cybersecurity. State-linked malware and cyber campaigns like Hacking Team's Remote Control System spyware[12], Pegasus[13], and the *Trident* zero-day exploit chain[14] demonstrated the powerful effect that cyber intrusions can play on individual human rights. These trends will only increase in frequency, and the U.S. must prepare to react and lead the way in thought leadership.

In a world where transactions are made in increasingly BYOD environments, current levels of encryption and security methods are always days-away from inferiority.[15] By spearheading the initiative for robust security standards and engaging the public in awareness campaigns, we have the potential to halt cyber intrusions before they ever occur, and shape the narrative for cyber engagement to come.

5 POLICY RECOMMENDATIONS

The government must **mandate cybersecurity controls and standards amongst government industries and contractors**—namely, the Top 5 of the 20 Center for Internet Security's Critical Security Controls. Controls like these will improve the general standards of cyber hygiene across all industries, and raise the technical bar across the board. The entire list of 20 controls will only become more relevant as cyber-attacks become more sophisticated and frequent, so it will be of vital importance to know what assets are on a network at all times.

The government must **funnel greater resources into cyber innovation and training**. Currently, the government is the leader in cyber research and development, but the majority of technical innovation capable of making a difference in the lives of civilians never makes it outside of the national labs. This can be accomplished through strategic use of existing mechanisms, like tech transfer programs. There is no need to reinvent the wheel in creating new technology for civilian use. The government should instead look at all the tech that's been funded over the last twenty years for cyber research and development. This represents one of the few tech areas where government is likely ahead of industry in most cases, and that tech benefits no one by sitting idly on a shelf. Further R&D should also be conducted with an eye towards commercialization, that way there is less layover time in the transfer from national labs to the private sector.

[12] Marczak, Scott-Railton, and McKune for CitizenLab, "Hacking Team Reloaded? US- Based Ethiopian Journalists Again Targeted with Spyware": https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/

[13] The Pegasus Software, Lookout Blog: https://blog.lookout.com/blog/2016/08/25/trident-pegasus/

[14] Marczak andScott-Railton for CitizenLab, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender": https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[15] AV-TEST Institute registers over 390,000 new malicious programs every day https://www.av-test.org/en/statistics/malware/

Tech policy should be crafted with an eye towards the intersection of cyber and human rights—this area is so amorphous and thorny that it has no established realm of ownership and few subject matter experts. With physical implications growing in connection to cyber-attacks, the government must anticipate sophisticated social problems by limiting the resources for committing crimes through the internet. While many people think about cyber, they don't think about the human rights side, precisely because many of these factors fall into others job descriptions and realm of influence. Major components of the government and private sector aren't tremendously sophisticated from cyber security problems, while others are helpful but stymied with limited jurisdiction.

A prime example of an existing program that has the potential to fit the needs of these recommendations is the Tech Transfer Program (TTP). TTP is woefully underfunded, but has demonstrated a lot of success. The only barrier holding these programs back is the limited funding to go out and discover more innovative solutions. The national government is good at sustaining solutions in the national labs and academic spaces, but hasn't looked at broader use an applications or SVIR grants to see what other sectors would contribute to this fight.

The next step towards tangible policy solutions is better funding these programs and helping to better promote their resources and personnel. So few government agencies know about and capitalize upon these resources—with programs like these already in place, it would be far more cost effective to tailor the tech transfer program to meet our current needs than go through the process to create new ones.

6 RECOMMENDATION DETAILS

The mechanisms by which we address these issues will pave the way for future success or failure in governance. Specifically, the United States government must consider and move to enact the following recommendations in order to stay ahead of the innovative rise in cyber-enabled crime.

6.1 PROMOTE RESILIENCY THROUGH BETTER CYBER HYGIENE PRACTICES

Despite the growing influence of cybersecurity and new outcrops of technology, the security of government network systems at every level are woefully inadequate on the whole, and largely fragmented at individual nodes. That is, there is little to no standardized system across the board for securing systems and updating standards. These weaknesses threaten the confidentiality, integrity, and availability of critical information and information systems used to support operations, assets, and personnel.[16]

[16] U.S. Government Accountability Office, *Key Issues: Cybersecurity* http://www.gao.gov/key_issues/cybersecurity/issue_summary

The government must use its purchasing power and influential status to set an example for other industries and regularity bodies. As we've seen in the past with other mandated regulations, enforcing minimum standards will make the entire industry increase its security because they will all be held to account for maintaining at least the same standards that the government has in place.

The government must move quickly and decisively to protect federal, state, and local enterprise systems with simple and essential cost-efficient solutions. The Center for Internet Security's (CIS) 20 Critical Security Controls provide an excellent framework for policymakers to build upon.[17] The checklist of standards and practices is easy to implement, automatable, and provides a foundation upon which public and private sector entities can scale up.

Of the 20 CSC, the Top 5 Controls provide specific and actionable ways to stop today's most pervasive and dangerous attacks by focusing on a smaller number of actions with high pay-off results.[18] When properly implemented, The Controls have the potential to reduce the risk of cyberattack by around 85-percent.[19] Leadership at all levels must move to enforce implementation of these controls, and include them in broader educational materials.

The U.S. must also strengthen and empower bodies like the Internet Corporation for Assigned Names and Numbers (ICANN), who ensure the internet's stable and secure operation. Groups like ICANN also have credibility in other nations where the U.S. does not. In supporting external NGOs, the internet can be governed by multinational bodies and will have broader representation and standardization requirements.

6.2 ENCOURAGE TECH TRANSFER PROGRAMS

As it stands, the U.S. government leads all other sectors in terms of technical innovation in cyber security because of its military applications. Individual agencies have found limited success in in transitioning federally funded cybersecurity technologies to the private sector, but none have been as successful as the Department of Homeland Security Cyber Security Division (CSD) Transition to Practice (TTP) program.[20]

[17] CIS Critical Security Controls for Effective Cyber Defense https://www.sans.org/critical-security-controls

[18] In 2010, John Streufert, Chief Information Officer of the U.S. State Department, demonstrated a more than 94-percent reduction in measured security risk by implementing the 20 CSC—thus earning him a Federal 100 award and promotion to become the head of DHS' National Cybersecurity Division. https://www.sans.org/reading-room/whitepapers/analyst/reducing-federal-systems-risk-20-critical-controls-35235

[19] Center for Internet Security https://www.cisecurity.org/critical-controls.cfm

[20] DHS Science and Technology, TTP Summary https://www.dhs.gov/science-and-technology/csd-ttp

TTP's explicit goal is to prepare for next-generation cyber threats, and since its inception in 2012, it has successfully transitioned eight federally funded cybersecurity technologies to the private sector for commercial offering.[21] Each year the TTP program selects a handful of promising cyber technologies to incorporate into its 36-month program. DHS' Science and Technology Directorate (S&T) introduces these technologies to end users around the country with the end goal of transitioning them to investors, developers or manufacturers that can advance them and turn them into commercially viable products.[22]

Through TTP, S&T does most of the leg work to identify, provide, and seed funding for research and development of next-generation technologies—the private sector need only complete the cycle by stepping up and providing guidance and resources for commercial usage.[23] An approach like this would likely find success in the federal contracts market place, and can be adapted to fit the same guidelines as those contracts bid out through regulated federal procurement practices.

The mechanism for improving cyber security for civilian usage already exists—there is no need to reinvent the wheel in scrapping existing R&D to fund de-classified projects. The government should instead look at all the technology it has created and stockpiled, and move quickly to transition it to the private sector via TTP initiatives. Programs like TPP, the Small Business Innovation Research (SBIR)[24] and Small Business Technology Transfer (STTR)[25] need to be better advertised throughout components to normalize usage and institute an environment of collaboration between government agencies and the private sector.

In the future, R&D should also be conducted with an eye towards commercial applications, that way there is less lag-time in the transfer from national labs to commercial markets. Instead of identifying projects for commercial use at the end stage of research and development, government groups should work to fund and encourage projects that are immediately applicable to commercial use. This will help to offset the amount of time that is taken to de-classify projects, safeguard sensitive information and intellectual property, and pass chain-of-command duties off to private entities.

[21] Cyber Security Division Transition to Practice Technology Guide, FY 2016: https://www.dhs.gov/publication/fy16-ttp-tech-guide
[22] ibid
[23] ibid
[24] https://www.sbir.gov/
[25] Agencies outside the cybersecurity space have already developed successful models of transition between the government and private sector. A fantastic example is the SBIR/STTR exchange program with the National Institutes of Health, which work to share information on life-saving scientific discoveries: https://sbir.nih.gov/about

Tech transfer programs represent the way forward because they have a greater net effect on society than the sum of their economic and scholastic gains; programs like DHS' TTP are beneficial because they develop better lines of communication between researchers and the investment community to fund activities that better serve our society. The goal of the TTP program is not only to accelerate the transition of cybersecurity research, but also to build lasting connections and processes that can be adopted by others to become self-sustaining.[26]

6.3 STRENGTHEN HUMAN RIGHTS PROTECTIONS IN POLICY

The internet and the plethora of devices it is linked to is a powerful tool to both connect people across countries and continents, as well as to exploit and harm them. We as a country are trying to promote US interests but also the interests of human rights globally, and where possible, we should promote efforts to protect vulnerable minority populations in the increasingly connected physical- and virtual-worlds.

In addition to the provisions made here for good cyber hygiene and innovation with respect to individual human rights, future leadership will be forced to confront issues of statehood and international organizations. Namely, the U.S. must prepare itself to confront growing concerns surrounding internet censorship programs (particularly regarding political dissidents), and state-sponsored cyber espionage and attacks. In this respect, the U.S. government must work with its allies to insure the following at the highest levels:

A standard of accepted procedure in the international community regarding cyber boundaries—against other states, and against a state's private citizens. Albeit a broad definition with contentious scope and depth, there are starting points for adapting official policy. Both the Reform Government Surveillance (RGS) [27] procedures and the Manilla Principles[28] represent a good outline for standardizing procedures, that are already widely endorsed by civil society groups around the world. They offer frameworks that can be tailored to fit the needs to both the public and private sector, with the added benefit of enabling the environment for innovation while protecting freedom of expression.

[26] Cyber Security Division Transition to Practice Technology Guide, FY 2016: https://www.dhs.gov/publication/fy16-ttp-tech-guide

[27] Reform Government Surveillance, https://www.reformgovernmentsurveillance.com/

[28] Manilla Principles on Intermediary Liability, https://www.manilaprinciples.org/

Agreement on accepted norms vis-à-vis state-state spying, specifically those that ensure clear understanding of when rules have been broken or spying as gone too far, when it affects our critical infrastructure, or when benign surveillance crosses the line into stealing intellectual property or commercial resources. Although not a perfect solution, bilateral lines of communications like those represented in the October 2015 U.S.—China Cyber Agreement represent important steps towards establishing boundaries and mutually-beneficial information sharing.[29] International agreements are inherently difficult to enforce and agree upon, but by providing a standard road map for relationship building, the U.S. can offer actionable steps in pioneering solutions.

On an international scale, the U.S. should encourage Internet Service Providers (ISPs) to use notice and takedown policies with greater frequency—which assists in identifying real abuses of freedom of speech, while shielding intermediaries from liability for third-party content. These policies can be used in tandem with economic incentives (namely, sanctions) to enforce cooperation. Financial retaliation is more likely to be effective to defeat cross-border cyber-enabled terrorism in practice compared to other forms of penalties. Specifically, the U.S. government could impose sanctions on foreign-owned companies that are helping to bolster offending nation's infrastructure and economy. Punishing banks and financial institutions that provide resources and support to North Korea would also significantly hurt the country's main economic ties. Hacker groups require financial support to operate and function.

7 CASE STUDIES

Technology has changed the fundamental nature of threats to human rights, and as a result, new problems have arisen that were never barriers before. In particular, technology has expanded the human trafficking scope and results in a multi-jurisdictional nature which poses challenges to policy responses. Moreover, an additional concern that arises when responding to cyber-enabled human trafficking is the delicate balance between privacy and civil liberties.

Privacy concerns also arise in this sort of discussion. More dialogue is needed to evaluate the role that increased privacy plays in individual's right to privacy; more specifically, to what extent are exploitation of individuals a byproduct of increased privacy? The internet and mobile technology allows individuals to maneuver in undetectable ways and policy leaders need to address this intersection between privacy and human trafficking.

[29] U.S.—China Cyber Agreement, October 2015 https://www.fas.org/sgp/crs/row/IN10376.pdf

7.1.1 Child Sexual Exploitation

Child sexual exploitation is a little understood and commonly overlooked crime that occurs around the globe. More recently, the reach of this criminal network has increased dramatically, thanks to the growth of cyber sophistication, a decrease in the cost of access, and an increase in relative anonymity. Although this topic is quite heinous, it is a reality and a real danger that all families face. The sexual exploitation of children through information and communication technologies is a known challenge, but not enough has been done to combat it. Critical steps must be taken to protect children everywhere and promote their human rights.

Considering this potential for an increase in child exploitation crime, it is important to focus efforts appropriately. Much of the current discussion regarding the online sexual exploitation of children focuses on educating children to protect themselves against online enticement for sexual interactions. While it is certainly important to educate children about how to remain safe online, the ICE maintains statistics which reveal that 75 percent of children subject to online sexual exploitation are pre-pubescent children. This is mirrored in a report from the Council of Europe Data Protection and Cybercrime Division stating that 74 percent of child victims in 2010 were under the age of 10, a percentage that has shown steady growth with each passing year.[30] Furthermore, 50 percent of that group represents infants and toddlers— children who are at risk not because they engage in online activities irresponsibly, but because they are in some way under the care or supervision of sexual predators. In fact, parents and custodians commit most online child exploitation crimes.

Outside of the purview of the Budapest Convention, the *Convention on the Protection of Children* provides for preventative measures, victim assistance, criminalization of child sexual abuse, protecting children in criminal proceedings, international cooperation, holding nationals accountable for offenses, and the participation of all sectors in the prevention of these crimes. In addition, the Council of Europe, through the Global Project on Cybercrime, also supports any interested countries in their efforts to combat this rampant crime. The project aims to ensure implementation of the *Budapest Convention* by strengthening, among others, cyber-enabled crime policy, ISP cooperation, and data protection.[31] Each of these treaties is designed to strengthen the others, but the world is far from overcoming the challenge posed by this powerful criminal network and the repugnant work that it does.

[30] Data Protection and Cybercrime Division. "Protecting Children against Sexual Violence: The Criminal Law Benchmarks of the Budapest and Lanzarote Conventions." *Global Project on Cybercrime*. Council of Europe, 4 Dec. 2012.

[31] "Protecting Children against Sexual Exploitation and Abuse."

Another unit dedicated to fighting against child exploitation is Homeland Security Investigation's (HSI) Child Exploitation Investigations Unit. HSI strives to protect children around the globe with its creation of Operation Predator, an international initiative to find and arrest child predators that draws on the agency's investigative and enforcement authorities. Its work includes a close study of antiquated methods of child sexual exploitation image sharing and a mission to understand the sharing of illegal images and videos online, which is an international crime, given that the Internet is borderless. HSI has the ability to collaborate with more than 70 offices overseas, and their law enforcement partners, enabling it to bring together ample resources to target child predators. This agency serves as the U.S. representative to the Interpol working group that locates new materials online and refers them to affected countries.[32] In intention, HSI is headed in the correct direction, but more must be implemented to effectively combat child sexual exploitation.

Among other international instruments, it is also important to mention the *UN Convention on the Rights of the Child (CRC),* which spells out protection standards to which children are entitled, including protection from exploitation. As one of nine core human rights treaties, it is almost universally ratified and requires that all states involved provide "appropriate legislative, administrative, social, and educational protective measures to ensure the child's safety from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment, or exploitation, including sexual abuse." States are also required to have social programs to provide support to affected children and anyone caring for those children.[33]

It is critical that any multilateral approach to be effective, it must focus on true, actionable items that advance the efforts of existing initiatives. Attention must be paid in four lacking areas:

- Funding
- Law enforcement
- International cooperation, and
- Awareness.

In terms of funding from a U.S. policy perspective, it is imperative that Congress increase the budget of HSI. HSI and ICE can work on formalizing detailed plans of what they would do with newly appropriated funds, as they already keep record of affected youth statistics and would be the most knowledgeable source for effective funding allocation. Some of these funds, and the expertise of HSI, should be dedicated to forming a formal working group within the U.S. that focuses solely on this issue and collaborates constantly with the UN.

[32] "Child Exploitation Investigations Unit." *Investigating Illegal Movement of People and Goods*. U.S. Immigration and Customs Enforcement, 2015.

[33] "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children." *Commission on Crime Prevention and Criminal Justice* (2014). United Nations Office on Drugs and Crime, 7 May 2014.

Second, this funding should in large part be dedicated to assigning increased law enforcement to focus on the challenge of child sexual exploitation online. Increasing the number of these agents by even a small percentage should make a noticeable change in the ability of the U.S. and other countries to locate and prosecute child offenders. Currently, many countries rely on tip lines and self-reporting from citizens. While these voluntary methods should not be discounted, it is crucial that there be law enforcement agents specifically focused on hunting down these perpetrators. With this background research in hand regarding other entities approach to policing, the U.S. could join together with other major powers interested in forming a joint task force. If a representative group of countries engaged in this initiative—say, the U.S., Europol, India, China, Brazil, Mexico, and Nigeria—it would be possible to create a collaborative task force that stretches across most of the globe. This initiative would be affordable and beneficial to all countries involved, both for their citizens' safety and their own internal approval ratings.

Continuing this notion of international cooperation, the third step would involve forming strong international relationships to combat predators unrestricted by physical borders. Currently, many countries engage in their own attempted awareness campaigns—although there is disagreement about their effectiveness—and law enforcement efforts. Since this type of crime is borderless, international collaboration is essential. A multilateral relationship, for example, between the U.S., China, Europol, and India would exert a lot of force in the world of foreign affairs. With each of these giants standing behind a common cause, it is conceivable that other countries would elect to join in the movement. Some existing treaties, while open for accession by any country, do not pressure any countries to join in support. Therefore, it is imperative to pressure these four powerhouses and design clear incentives for their accession, as well as disincentives associated with a decision to refrain. With this multilateral relationship in place, a first step would involve some aspect of double criminality.

Fourth, the power of increased awareness and advocacy in the U.S. cannot be underestimated. While this advocacy would ultimately be aimed at the American public, who currently knows very little about the reach of child sexual exploitation crimes online, advocacy efforts should first be focused on pressuring organizations such as the Ford and Rockefeller Foundations to carry out massive public affairs campaigns. These campaigns could highlight the stories of survivors, interested religious groups, or grieving mothers, and should focus on making the observers feel more intimately affected by these offenses. With these and other foundations' support, coupled with increased funding from Congress, it would be possible to educate more American constituents. These constituents would then be instrumental in pressuring policymakers to take action to prevent future crimes. Together, these four steps will bring a plan to weaken a thriving criminal network online closer to fruition.

Existing initiatives like the Budapest Convention on Cybercrime[34] and the Convention on the Protection of Children[35] have already identifies cyberspace as the next frontier for the exploitation of individuals, and have made preliminary steps towards strengthening cyber-enabled crime policy, ISP cooperation, and data protection. In order to maintain relevance as a leader in global influence, the U.S. government must focus on actionable items to advance the efforts of existing initiatives, and increase cross-department coordination. This means that the government should work to solidify policy that provides for increased law enforcement funding and resources; with the specific mission of locating and prosecuting cybercriminals, and training in new surveillance and monitoring techniques.

7.1.2 Human Trafficking

Human trafficking is another issue that has existed long before the advent of the internet. Governments in turn have responded with international, regional, and nation treaties and conventions in attempts to combat it, including the *United Nations' Convention against Transnational Organized Crime and the Protocols Thereto*[36] and the *United States' Trafficking Victims Protection Act* (2000)[37] .

Traffickers increasingly use the internet to facilitate trafficking through social media, discussion forums, advertisements, etc. Additionally, mobile phones are a useful tool for traffickers in creating new methods of exploitation that weren't previously available.[38] In particular, travel exchange-trafficking was never possible pre-internet—it is only with the rise of technology that these new forms of trafficking exist. So while human trafficking always existed, this added dimension of technological advancement fundamentally altered the nature and scope of the problem.

Cyber-enabled human trafficking is an issue of cyber resiliency. In essence, cyber-enabled human trafficking requires a practical response that is able to prepare and adapt to changing cyber conditions.[39] Combatting cyber-enabled human trafficking requires the ability to withstand and recover from continued human trafficking incidents enabled by technology. The human rights implications of trafficking, including violations of the right to life and various social and economic rights, are troubling and unacceptable. In response to this recognition, this memorandum analyzes the key players involved in combatting trafficking, discusses how to decrease incidences of cyber-related trafficking, and proposes recommendations for implementation.

[34] Treaty No. 185, Convention on Cybercrime: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[35] Convention on Protection of Children and Co-Operation in Respect of Intercountry Adoption: https://www.hcch.net/en/instruments/conventions/full-text/?cid=69

[36] "United Nations Convention against Transnational Organized Crime and the Protocols Thereto." *United Nations Office on Drugs and Crime*, United Nations. 2015.

[37] "Victims of Trafficking and Violence Protection Act of 2000." *US State Department*. 28 October 2000.

[38] "Summary of Key Findings, Further Research, and Guiding Principles." *Technology & Human Trafficking.* USC Annenberg Center on Communication Leadership Policy. 2015.

[39] "What is Security and Resilience." *Critical Infrastructure Security.* US Department of Homeland Security. 17 September 2015.

In the case of trafficking across the U.S-Mexico border, The resolution to human trafficking and more broadly, as mentioned in the TVPA, is three-pronged: 1) prevention of human trafficking and victim identification, 2) protection of human trafficking victims, and 3) prosecution of traffickers. However, whereas current efforts are still technologically lagging behind traffickers, this three pronged approach needs to be fundamentally changed to adapt to the shifting environment that creates a platform for cyber-enabled human trafficking.

The first prong of prevention and identification will predominantly involve training key players in techniques that allow them to monitor traffickers and victims online and across the internet. Moreover, it will require that key players remain up-to-date with the latest technology and how it may be used to traffic victims across the border. It is not enough to merely catch traffickers; the Mexican and American governments also have a responsibility to protect victims before and after trafficking. The protection of human trafficking victims requires adequate provision of necessary resources and safe spaces for victims to reengage with society and live their lives free from fear. The final prong in responding to cyber-enabled human trafficking is the prosecution of traffickers; this requires the quick and effective prosecution. Additionally, governments should ensure that appropriate punishments are given to traffickers. For those affected, human trafficking has severe consequences and perpetrators of trafficking should be given fitting punishment.

Human trafficking is a cross-national human rights problem, and so requires multiple players and stakeholders' engagement in order for any policy response to be effective. The primary players in the response to cyber-enabled human trafficking in this case include the involved national and affected- state governments, local and national law enforcement, and the general population—specifically NGOs, private corporations, the civilian population, and the victims themselves.

Combatting cyber-enabled human trafficking requires a multifaceted response and in-depth coordination between the stakeholders previously mentioned. However, such joint action risks potential problems regarding communication, poor planning, and misalignment of goals among and between the relevant players may result in poor implementation of the policies needed to combat online trafficking using the three-pronged approach.

8 IMPLEMENTATION

This commentary acknowledges the logistically challenging nature of these recommendations. In particular, resource constraints including limited financial resources and infrastructure pose significant potential problems. However, this commentary reemphasizes the importance of these recommendations and encourages all key players to implement these measures to the best of their capabilities and to the full extent of their resources.

Accordingly, we recommend the following 30/60/90 implementation plan for making steps towards actionable policy implementation. Based on the above policy recommendations, we believe that the next incoming President could begin to implement such policy in the first 100 days of office.

Regarding cyber hygiene and Critical Security Controls:

- Within the first 30 days, the President should issue and Executive Order mandating that all federal agencies and contractors must implement the Top 5 CSC.
- Within the first 60 days, the President would then begin a review process of each agency to see which contracts need to implement hygiene controls in order of importance. This review process would also outline a timeline plan by which each agency must comply.
- Within the first 90 days, the President would assign a component like US CERT or NCCIC to pilot assessments of all agencies and major contractors to ensure that they have implemented the controls. A fair amount of the logistics to implement this strategy have already been outlined in Tony Scott's Cyber Sprint.

Regarding R&D and tech transfer:

- Within the first 30 days, the White House should request briefings from the TTP on all research and development that's being commercialized today, and inventory what exists that has not yet been assessed. The next President would also be briefed on all technology in the process of transitioning.
- Within the first 60 days, the President should request a full audit of all the other technology that is not currently being transitioned, that could potentially apply to cybersecurity. The SBIR/STTR provides a wealth of existing ideas.
- Within 90 days, the White House should have a full program in place to begin the transition and expedition of technology licensing. Emphasis should be placed on that tech which is deemed both useful for private sector AND government, and has the capacity to automate the Top 5 Controls.

Regarding policy that is conscious of human rights:

- Within 30 days, the President should commission a working group to critically examine what the U.S. can do in cyberspace to support minority groups, political dissidents, and women and children that live in countries under oppressive regimes.
- Within 60 days, the President should head up an additional commission investigating abuses of the human rights of the most vulnerable in our society online. The commission should inform the president of three things:
    - Which agencies and sub-agencies are involved in combatting human trafficking, child pornography, and persecution of at risk communities online.

    - An assessment of non-US entities who are also involved in combatting human trafficking, child pornography, and abusing at-risk communities online.
    - Recommendations on how the U.S. can better integrate its efforts, and more effectively work with their partners in the private sector and abroad.
- Based on the commission's report, within 90 days, the President should issue an Executive Order which is informed by those findings. At the same time, he/she should ask Homeland Security Investigations (HSI) on how it will dramatically scale-up its efforts to meet the threats we face online. For example, since 2007, watchdog agencies have reported a 5000% increase in incidences of suspected child sexual abuse imagery. [40] In kind, the HSI and other policing agencies must prepare a plan to increase in size on the same order of magnitude. Once they have an idea of the measurements necessary, the White House must assist in crafting policies for next steps.

9 CONCLUSION

It is clear that the growth of technology used across a wide spectrum of industries poses dynamic threats to the security of organizational systems and personal information. The internet and the plethora of devices it is linked to is a powerful tool to both connect people across countries and continents, as well as to exploit and harm them. Ultimately, cyber security is a vital issue which leaders and civilians alike must become more proactive and aware of.

These recommendations remind us that cybersecurity issues faced by professionals, policy makers, and citizens are everywhere, and in almost everything we do. It recommends more resources, attention, and political effort be invested into cyber security measures and policy interventions to ensure the protection of the human rights of the billions of people online. We see that awareness is an overarching first step in many of the different cyber issues. Thus, creating a collective consciousness around our use of the Internet and connected technologies is an essential starting point. The tangible implications of cyber threats and the persistence of cyber-enabled crime is incredibly detrimental to society. Currently, far too many criminals are able to hide behind puzzles of proxy servers and commit felonies, confident that our lack of global coordination and awareness to the true threats they pose will keep them safe.

[40] NCMEC reviewed 22 million images and videos of suspected child sexual abuse imagery in its victim identification program in 2013 — more than a 5000% increase from 2007. https://www.wearethorn.org/child-pornography-and-abuse-statistics/

The United States, along with other influential countries and entities such as the United Nations, must bring the issue of cyber security to the public stage more forcefully. In the mean-time, it is also necessary that people continue to research the relevance of cyber threats in many different policy fields as well as industries. Although there is a long way to go, many gains can be made in cyber security both domestically and through cooperation with our fellow online nations, and those about to come online, to ensure that the Internet is as safe a place as possible where individual rights and liberties are honored.