



# **#CyberspaceIRL: Rule of Law Approaches to Virtual Threats**

**MAY 2019**

**American Bar Association Rule of Law Initiative Issue Paper  
Mary Greer and Tara Mobaraki**



AMERICAN **BAR** ASSOCIATION

---

Rule of Law Initiative



The statements and analysis expressed in this paper are solely those of the authors. The Board of Governors of the American Bar Association (ABA) has neither reviewed nor sanctioned its contents. Accordingly, the views expressed herein should not be construed as representing the position or policy of the ABA. Furthermore, nothing contained in this paper is to be considered as rendering legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel.

ISBN (print): 978-1-64105-510-9  
ISBN (e-book): 978-1-64105-511-6

Printed in the United States of America

Copyright © 2019 by the American Bar Association  
1050 Connecticut Avenue, NW, Suite 450, Washington, D.C. 20036

## American Bar Association Rule of Law Initiative

*Promoting justice, economic opportunity and human dignity through the rule of law*

1050 Connecticut Avenue, NW, Suite 450  
Washington, DC 20036, USA

phone: +1.202.662.1950  
fax: +1.202.662.1597

e-mail: [rol@americanbar.org](mailto:rol@americanbar.org)  
website: [www.abaroli.org](http://www.abaroli.org)



### 2018–2019 Board Members

Hon. M. Margaret McKeown, Chair  
Roula Allouch  
Don S. De Amicis  
Hon. James E. Baker  
Hon. Rosemary Barkett  
Peter V. Baugher  
Paulette Brown  
Hon. Judith Chirlin  
Laura Farber  
Robert Grey  
Glenn Hendrix  
Homer E. Moyer, Jr.  
Hon. Carolyn S. Ostby  
Ed Potter  
Beverly J. Quail  
Steven M. Richman  
Lauren Stiller Rikleen  
Hon. Lee H. Rosenthal  
Hon. Ramona G. See  
Wendy Shiba  
Walter H. White, Jr.

### Special Advisors

Hon. Stephen G. Breyer  
Michael Flowers  
Sharon S. Gerstman  
Hon. Ruth Bader Ginsburg  
David S. Jonas  
Hon. Anthony M. Kennedy  
Karen J. Mathis  
Llewelyn G. Pritchard  
Hon. Stephen J. Rapp  
James R. Silkenat  
Deanell R. Tacha  
Hon. James Wynn Jr.

**ABA Board of Governors Liaison to ABA ROLI**  
Myles V. Lynk

### Staff

**Alberto J. Mora**  
Director

**Jeff Borns**  
Deputy Director

**Sebastián Albuja**  
Director, Africa Division

**Elisabeth Baraka**  
Director, Asia and the Pacific Division

**Alexandra Belenkaya**  
Director, Europe and Eurasia Division

**Nerea Aparicio**  
Director, Latin America and the Caribbean Division

**Angela Conway**  
Director, Middle East and North Africa Division

**Paul Fisher**  
Director, Strategic Partnerships and Institutional Advancement

**Linda Bishai**  
Director, Research, Evaluation, and Learning

**David Dettman**  
Director, Outreach

**Dan Andresen**  
Director, Security

**Vladimir Gurin**  
Director, Finance

## ABOUT THE AMERICAN BAR ASSOCIATION

### RULE OF LAW INITIATIVE

For more than 25 years, and through our work in more than 100 countries, the American Bar Association Rule of Law Initiative (ABA ROLI) and our partners have sought to strengthen legal institutions, to support legal professionals, to foster respect for human rights and to advance public understanding of the law and of citizen rights.

In collaboration with our in-country partners – including judges, lawyers, bar associations, law schools, court administrators, legislatures, ministries of justice, and human rights and civil society organizations – we design programs that are responsive to local needs and that prioritize sustainable solutions to pressing rule of law challenges. We employ rigorous and innovative monitoring and evaluation approaches in assessing the quality and effectiveness of our programs.

ABA ROLI has roughly 500 professional staff working in the U.S. and abroad, including a cadre of short- and long-term legal specialists, volunteers, interns and third-party contributors.

## Table of Acronyms

Asia Internet Coalition	AIC
Children’s Online Privacy Protection Act	COPPA
Clarifying Lawful Overseas Use of Data Act	CLOUD Act
Commodity Future Trading Commission	CFTC
Communications Decency Act	CDA
Computer Emergency Readiness Team	CERT
Computer Fraud and Abuse Act	CFAA
Computer Service Providers	CSP
Convention on Cybercrime of the Council of Europe	Budapest Convention
Convention on International Trade in Endangered Species of Wild Fauna and Flora	CITES
Department of Justice	DOJ
Electronic Money Institutions	EMI
European Union	EU
Family Educational Rights and Privacy Act	FERPA
Federal Trade Commission	FTC
Financial Action Task Force on Money Laundering	FATF
G7 24/7 Cybercrime Points of Contact	24/7 Network
General Data Protection Regulations	GDPR
Health Insurance Portability and Accountability Act	HIPAA
Information and Communications Technology	ICT
Initial Coin Offerings	ICO
International Covenant on Civil and Political Rights	ICCPR
International Foundation for Electoral Systems	IFES
Islamic State of Iraq and Syria	ISIS
Mutual Legal Assistance Treaty	MLAT
National Security Agency	NSA
Nongovernmental Organizations	NGOs
Regulation of Investigatory Powers Act	RIPA
Stored Communications Act	SCA
United Nations Convention against Transnational Organized Crime	UNTOC
Verified Internet Pharmacy Practice Sites	VIPPS
The Vulnerabilities Equities Process	VEP

## Table of Contents

<b>Table of Acronyms.....</b>	<b>5</b>
<b>Foreword.....</b>	<b>6</b>
<b>Acknowledgements .....</b>	<b>7</b>
<b>Introduction.....</b>	<b>8</b>
<b>International Legal Frameworks .....</b>	<b>9</b>
The Budapest Convention .....	10-11
U.S. Framework.....	11-12
Cyberspace Solarium Commission .....	13
Strategies Across the Globe .....	13-14
<b>Enforcement .....</b>	<b>15</b>
Personal Jurisdiction Over Perpetrators .....	15
Collection of Evidence.....	16
Processes .....	16-17
Private Sector .....	17-18
<b>Election Security.....</b>	<b>18-19</b>
Measures to Counter Election Interference .....	19
Election Security Worldwide .....	19-20
<b>Virtual Currencies .....</b>	<b>20-21</b>
Using Bitcoin to Counter Sanctions .....	21
Terrorism .....	21-22
Money Laundering .....	22
<b>Trafficking and Crime Convergence.....</b>	<b>23</b>
Wildlife Trafficking .....	23-24
Human Trafficking .....	24-25
Drug Trafficking .....	25
<b>Internet Freedom.....</b>	<b>25-26</b>
The International Covenant on Civil and Political Rights .....	26
South Asian Countries.....	26-28
Comparison of Penalties Chart.....	28
<b>Incitement.....</b>	<b>29</b>
Social Media as the problem.....	29-30
Hate Speech Affecting the Muslim Population .....	30-31
<b>Conclusion.....</b>	<b>31</b>
<b>Endnotes .....</b>	<b>32-36</b>

## FOREWORD

The ABA Rule of Law Initiative (ABA ROLI) put together this study in its Paper Series to bring attention to the contributions rule of law actors can make in addressing cyber threats and challenges. With increasing vulnerability and the magnification of scale for criminal activities enabled by cyber platforms, it is critical to engage all relevant actors for a comprehensive response. Support for the rule of law can involve promoting responsible and effective legislation, providing training in appropriate rights protections and criminal justice responses, and expanding citizen awareness. This paper reviews the relevant legal frameworks, highlights some of the gaps, and identifies concrete steps that may be taken to maximize effective responses to cyber threats.

This study serves as a companion to ABA ROLI's 2019 Annual Conference on Contemporary Rule of Law Issues, "#Cyberspace IRL: Rule of Law Approaches to Virtual Threats," convened on May 21, 2019 in Washington, D.C. in collaboration with the United States Institute of Peace, the ABA Standing Committee on Law and National Security, and the ABA Section on Criminal Justice. The conference brings together a diversity of stakeholders, drawn from the development, legal, official, business, and academic communities to dive into these complex issues, share collective experiences, and inform policy development. Videos of the conference panels and keynotes will be available on the ABA ROLI website at [ambar.org/cyberspaceirl](http://ambar.org/cyberspaceirl).

ABA ROLI is pleased to lead this effort as part of our commitment to sharing insights gathered from over 25 years of experience in developing the rule of law. Our mission is to promote justice, economic opportunity, and human dignity through the rule of law. As this mission suggests, we see the rule of law as a means to an end, a critical tool for solving global problems; the contemporary challenges and proliferation of threats in cyberspace are a prime example.

We are grateful to the authors for their contribution to this effort and look forward to ongoing learning through our 2019 conference and beyond. For more information about this work, please contact ABA ROLI Director of Research, Evaluation and Learning Linda Bishai at [linda.bishai@americanbar.org](mailto:linda.bishai@americanbar.org).



M. Margaret McKeown  
Chair, ABA ROLI Board of Directors



Alberto Mora  
Director, ABA ROLI

## Acknowledgements

This paper was co-authored by Mary Greer, Senior Technical Advisor in the Research, Evaluation and Learning Division at the American Bar Association Rule of Law Initiative (ABA ROLI) and by Tara Mobaraki, research intern at ABA ROLI. The authors wish to cordially thank the ABA ROLI Board of Directors, the ABA ROLI Program Committee, ABA ROLI staff and interns, and members of the issue conference working group for their invaluable support during the research, writing, and editing of this paper. Special thanks are extended to Diana Thomson, Samantha Tu, Lorraine Greer, and Hope Ann Roberts for their critical logistical assistance in the formatting and publication stages.

Special thanks are extended to Jeffrey Borns and Linda Bishai for ongoing guidance and constructive critique of ideas and content. The authors are extremely grateful for the time and assistance rendered by content reviewers and experts who contributed to the drafting of this paper but who wished to remain uncredited. Their contributions were deeply appreciated.

## I. INTRODUCTION

The hyper-advancement of information sharing technologies in recent decades has provided unprecedented opportunities for enhanced connections and communications across the world, but serious challenges have accompanied these advancements. Those challenges are perhaps most acute when addressing cyber security issues. To contribute to the international discussion and response to the complex issues surrounding cyber security, the American Bar Association Rule of Law Initiative (ABA ROLI), has chosen to focus discussions at its Third Annual Conference on Contemporary Rule of Law Issues on this topic. ***#Cyberspace IRL: Rule of Law Approaches to Virtual Threats***, convenes a diversity of stakeholders in the cybercrime policy arena, connecting the legal and rule of law development communities with donor agencies and the private sector for cross-sectoral discussions, exchanging lessons learned and articulating a shared agenda for addressing the rule of law dimensions of cybercrime. This conference paper serves to highlight relevant background information related to each of the conference subtopics to assist the reader to begin to delve into an area of interest. No one section is intended to be entirely comprehensive but provides an overview of each subtopic. The rule of law issues prioritized in the conference discussions include:

- an examination of global legislative frameworks and conventions primarily related to the Budapest Convention;
- enforcement challenges particularly with convergent crimes like money laundering and trafficking, which can also be furthered using virtual currency;
- governmental overreaches that restrict freedom of speech and association, as well as the dangerous use of virtual spaces to incite violence; and
- election security and the erosion of trust in democratic institutions.

Lastly, while rule of law implementers often partners with and support justice actors in addressing these issues, the paper will identify the breadth of actors and partners outside the traditional rule of law arena, including from civil society and the private sector, who by necessity must be part of devising and implementing effective strategies and solutions.

## 1. International Legal Frameworks

Effectively addressing cyber security challenges requires consistent adherence to international conventions and protocols, and best practices, as well as a confluence of criminal and regulatory reform. However, the only binding international instrument on this issue is the **Convention on Cybercrime of the Council of Europe**<sup>1</sup>, (more commonly known as the **Budapest Convention**). The Convention is not a consistent or globally applied law, nor does it automatically come into effect, its protocols and guidance notes serve as a legal framework for any country developing comprehensive national legislation against cybercrimes, and as a framework for international cooperation between State Parties to this treaty. Guidance Notes further refining the implementation of the Convention reflect the quickly changing landscape since its coming into force in 2003. Current guidance note discussions are addressing the access to and use of evidence in the Cloud, as well as providing much needed protocols for emergency mutual legal assistance. There are also ongoing discussions regarding a possible additional protocol to the Budapest Convention, which may seek to expand the treaty in several important ways, including possible new articles on international cooperation, direct cooperation with service providers and transborder access to data. Other important frameworks include:

- **The United Nations Convention against Transnational Organized Crime (UNTOC)** and its protocols also provide mechanisms for international cooperation to combat transnational organized crime, including cybercrimes.<sup>2</sup>
- **The African Union Convention on Cyber Security and Personal Data Protection**<sup>3</sup>, which follows many of the provisions of the Budapest Convention.
- The **G7 24/7 Cybercrime Points of Contact (24/7 Network)** is an initiative that promotes practical cooperation among law enforcement.<sup>4</sup>
- The **General Data Protection Regulations (GDPR)**, enacted in 2016 but enforced as of May 25, 2018, regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.<sup>5</sup>

Many countries, especially signatories to both the **Budapest** and the **UNTOC Conventions**, have enacted legislation and procedures addressing these crimes. But given its complicated nature and global breadth, less developed or less independent legal systems are typically the weak link in global or regional efforts at prevention and enforcement. And finally, though existing instruments

like the **Budapest Convention** and the **UNTOC** provide helpful tools to combat cybercrime and the strengthening of national laws and building of cybercrime law enforcement capacity are becoming higher priorities, various governments and actors (including representatives from the private sector) are advocating

for the creation of a new global framework. These efforts range from a draft global treaty on information security promoted by the Russian Federation, to initiatives such as the “Geneva Declaration for Cyberspace” advanced by retired Norwegian judge Stein Schjolberg.<sup>6</sup>

In Peru, as part of its ongoing technical assistance to prosecutors, ABA ROLI published a **Manual on Digital Evidence** to assist law enforcement officials and prosecutors to more effectively gather electronic evidence, such as that involving pornography or credit card fraud.

## The Budapest Convention

The **Budapest Convention**, is, to date, the only binding international instrument that gives a legal roadmap to countries to strengthen their ability to investigate and prosecute cybercrime. The Convention has three main components:

- harmonizing the domestic criminal substantive law elements of offenses and connected provisions in the area of cybercrime;
- providing for domestic criminal procedural law powers necessary for the investigation and prosecution of traditional cybercrime offenses, as well as other offenses committed by means of a computer system or for which relevant evidence is in electronic form; and
- setting up a fast and effective regime of international cooperation.

### *Strengths:*

The value of the Convention as an international tool rests on its requirements that Parties have a basic level of domestic criminal law in the field and provide a platform for transnational law enforcement cooperation in investigations, evidence sharing, and extradition. While there is no globally accepted definition of cybercrime, the **Budapest Convention** is built on the premise that, despite differing legal systems and definitions, countries can and do agree on the basic nature of criminal activities that constitute cybercrime. By January 2018, 71 states were members or observers in the cybercrime convention committee, and 90% of UN member states have commenced reforms of some kind on cybercrime, compared to 74% since 2013. There is consistent progress in the growth of the treaty, with a growing list of developing countries publicly announced as in the process of accession, with a larger (and growing) number of countries requesting assistance in strengthening their laws to comply with the Convention in preparation to join. For example, the Congress of Peru just approved the act of accession to the **Budapest Convention**.<sup>7</sup>

### *Weaknesses:*

Opponents of the **Budapest Convention**, such as the People's Republic of China (China) and the Russian Federation (Russia) argue that provisions of the **Budapest Convention**, such as articles on trans-border access to data, are "violations of state sovereignty".<sup>8</sup> Russia is dissatisfied with the Convention, alleging that its provisions allow foreign law enforcement agencies to conduct investigations within signatories' borders using the internet.<sup>9</sup> China also argues from the perspective of asserting state sovereignty, advising they are concerned with the impact of the western multi-stakeholder model on its internal stability.<sup>10</sup> The U.S. and its allies argue that the Russian and Chinese definition of "harmonization" of global legal frameworks as requiring a new global treaty is misplaced, noting that the harmonization approach in Budapest recognizes that national laws need not be identical so long as countries' laws capture the core criminal conduct. The U.S. contends that the demand for "harmonization" instead masks the desire of countries like Russia and China to assert their own principles of authoritarian control over technology.<sup>11</sup>

While Brazil, Russia, India, China, and South Africa (the "BRICS" countries) continue to reject the Budapest Convention, and it is unlikely that Russia or China will ever join, there may be other factors driving their policy. Like China, Russia views the multi-stakeholder approach to technology as a threat to internal stability, while China also has a "long game" focus on asserting its influence through global expansion of the Chinese high-tech sector, particularly in cutting edge areas like artificial intelligence and 5G networks. Given the strategic importance of the BRICS alliance, it remains important to find areas where interests may intersect.

While the **Budapest Convention** remains the best existing tool for countries globally, there remains a great challenge regarding the capacity to enforce existing laws, even if they are strong and well-written. Uneven enforcement efforts are in most cases driven, especially in developing countries, by a simple lack of expertise and equipment, creating avenues of potential focus among donors and rule of law implementers. It also might be best to look for practical solutions instead of new treaties for which there is no global consensus, such as enhanced collaboration and cooperation between the public and private sectors, as well as augmenting cybersecurity resources.

## U.S. Framework

The United States did not have to alter its domestic laws to join the Budapest Convention, since it already had or eventually enacted relevant domestic legislation:

- I. The **Comprehensive Crime Control Act** enacted in 1984, included the **Computer Fraud and Abuse Act (CFAA)**.<sup>12</sup> The CFAA outlaws conduct that victimizes computer systems, protecting federal computers, bank computers, and computers connected to the Internet, shielding them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. Specifically, the **CFAA outlaws**:
  - computer trespassing (e.g., hacking) in a government computer, 18 U.S.C. 1030(a)(3);
  - computer trespassing (e.g., hacking) resulting in exposure to certain governmental, credit, financial, or computer-housed information, 18 U.S.C. 1030(a)(2);
  - damaging a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, a denial of service attack, and other forms of cyberattack, cybercrime, or cyber terrorism), 18 U.S.C. 1030(a)(5);
  - committing fraud an integral part of which involves unauthorized access to a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(4);
  - threatening to damage a government computer, a bank computer, or a computer used in, or affecting, interstate or foreign commerce, 18 U.S.C. 1030(a)(7);
  - trafficking in passwords for a government computer, or when the trafficking affects interstate or foreign commerce, 18 U.S.C. 1030(a)(6); and
  - accessing a computer to commit espionage, 18 U.S.C. 1030(a)(1).<sup>13</sup>
- II. The **Communications Decency Act of 1996 (CDA)** added **Section 230** to the **Communications Act of 1934**, generally protecting online service providers from legal liability stemming from content created by the users of their services, with some exceptions. Section 230(c)(1) states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”<sup>14</sup> Some have cited Section 230 as one of the most important provisions protecting free expression on the Internet because providers like Facebook, Twitter, and Google are permitted to publish others’ content without reviewing it for criminality or other potential legal issues. However, others argue that its liability protections are overbroad, and may facilitate sex trafficking and other criminal behavior by permitting online service providers to display advertisements for illegal activity without fear of liability.<sup>15</sup>
- III. The **Cybersecurity Information Act** passed by Congress in 2015, permits companies to share cyber threat indicators with the government, and liability protection for the

information they share with the Department of Homeland Security.<sup>16</sup> Due to negotiations and pushbacks with other proposed bills, the Cybersecurity Act had been in the making for some time.<sup>17</sup>

- IV. The **Clarifying Lawful Overseas Use of Data Act** (commonly known as the Cloud Act), was enacted to help with investigations and to force technology companies into providing data hosted abroad. One of the more important provisions requires a company under U.S. jurisdiction to produce data under its control.<sup>18</sup> Under the Cloud Act, U.S. government officials can enter into executive agreements with other countries to address conflict of law problems and even remove restrictions so that Computer Service Providers (CSPs) can comply with lawful orders.<sup>19</sup> The Cloud Act supports Article 18(1)(a) of the Budapest Convention, which requires parties to adopt national laws ensuring proper authorities to compel providers to disclose electronic data in their possession.<sup>20</sup>
- V. **The Vulnerabilities Equities Process (VEP)**: In accordance with paragraph (49) of National Security Policy Directive-54/Homeland Security Policy Directive-23, Cybersecurity Policy, and the *Joint Plan for the Coordination and Application of Offensive Capabilities to Defend U.S. Information Systems*, the USG created the VEP.<sup>21</sup> According to the Charter issued by the White House on March 15, 2017, the VEP “balances whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence.”
- VI. The 2018 **Department of Defense Cyber Strategy** represents the Department's vision for addressing this threat and implementing the priorities of the National Security *Strategy* and National Defense *Strategy* for cyberspace.<sup>22</sup> The strategies include building a more lethal joint force, contesting malicious cyberactivity in a day to day basis, strengthening alliances and attaining new partnerships, incorporating cyber awareness, and sustaining a cyber workforce. In his article, *“Between Hacks and Hostilities: Are the US government and private sector ready for persistent engagement?”* the Hon. James E. Baker commented that such strategies would be effective if the government is willing to use all instruments of national power to enforce cyber norms. He noted it is also imperative that the government is aware of the actions the private sector is taking, otherwise the government cannot form an effective plan to combat cybersecurity threats. Likewise, the private sector needs to assist the government by shaping policy outcomes.<sup>23</sup>

The U.S. government has also enacted important privacy laws such as the Children’s Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA).<sup>24</sup>

### Harmonizing Standards to Support a Cybernorm

ABA ROLI, in partnership with Moldovan civil society organization The Institute of Information Policy, participated in consultations with policymakers and other stakeholders to revise Draft Law 161, to ensure that regulations impacting Internet freedom were harmonized with European norms and standards; changes included more targeted restrictions on illegal content blocking and greater specificity in the categories of data that telecom service providers are required to store.

## Cyberspace Solarium Commission

Section 1634 of the National Defense Authorization Act, enacted on August 13, 2018, called for the creation of the Cyberspace Solarium Commission, which is responsible for implementing strategies against adversaries in cyberspace.<sup>25</sup> The 13-member commission will have the power to subpoena, and under this legislation, government cooperation is required from all agencies.<sup>26</sup> The commission is also required to submit a report that addresses strategic frameworks and how they address national security sector and political issues, how resources should be allocated, and whether the government structure should be revised.<sup>27</sup> Instead of being submitted to the President, the report will be submitted to the Director of National Intelligence, Defense Secretary and Homeland Security Secretary. On May 8, 2019, Senator Angus King and Representative Mike Gallagher announced that they will be leading the commission.<sup>28</sup>

### Obligation to Disclose Breaches

In November 2018, cyberhackers stole data from about 500 million customers, one of the largest known breaches of personal data. The attackers took contact information, travel and passport information. Evidence points to a Chinese intelligence group; however, China denied knowledge of the attack. Since then, Marriot has taken measures such as emailing affected customers, working with system vendors, and reviewing national and local regulations. The Marriott situation is an indicator for regulators and other companies, that disclosures continue to be inadequate, that mergers can trigger cybersecurity breaches, and that companies and their boards are still not prepared for cybersecurity breaches. Regulators can compel companies to be more prepared by requiring board of directors to be more transparent about cybersecurity exposure with shareholders, and increase corporate accountability so that damages, and especially risks to consumers, are mitigated.

Shivaram Rajgopal & Burga Gezer, *The Marriott Breach Shows Just How Inadequate Cyber Risk Disclosures Are*, Harvard Business Review, (March 5, 2019).

## Strategies Across the Globe

Worldwide, countries are attempting to implement and establish regulations to address cybercrime and privacy related issues.

- The EU has expressed concern regarding the Cloud Act because U.S. authorities could use the Act to require companies providing communication services to allow access to data stored outside the U.S., which could undermine the GDPR.<sup>29</sup> The GDPR places a fine of up to 4% of a company's revenue for violations and applies to foreign companies like Facebook as well.<sup>30</sup> The EU is attempting to force companies to prioritize privacy for an individual's personal information by mandating that customers be able to see and delete data that concerns them, by providing notice within 72 hours of a breach to customers, and by making data policies as transparent as possible to a layperson.<sup>31</sup> Companies located in the EU might have an easier time adjusting to the new set of requirements that the GDPR establishes, since previous privacy laws in the EU overlap with the GDPR.<sup>32</sup> Because the GDPR is still fairly new, many predict that regulators will give companies the benefit of the doubt if they act in good faith.

One of the most important, and perhaps complicated mandates, is the data breach notification. While a company is required to notify a customer regarding breached data within 72 hours, regulators are not sure how to protect those affected by the breach.<sup>33</sup> In the U.S., privacy laws are not as stringent and there are exceptions to notifying individuals when a breach occurs. Many other countries, such as Israel and Canada, have been following the EU's approach as well, which arguably could put U.S. companies at a global disadvantage.<sup>34</sup> As noted, the EU's laws protect personal data whereas in the U.S., jurisdictions have conflicting notice provisions, burdening the individuals whose information has been jeopardized to discern a course of action.<sup>35</sup>

In Europe and Eurasia, ABA ROLI has worked with local partners to develop and share educational materials for lawmakers on internet freedom principles under international law and draft template legislation to promote internet freedom.

According to the Telecommunication Union, countries that are best prepared against cyberattacks include Singapore, United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France, and Canada.<sup>36</sup>

- In 2007, **Estonia** had significant problems with a series of cyberattacks on official institutional networks, heralding a new era of cyberwarfare. In response, Estonia signed agreements for training and cooperative efforts with NATO, Austria, and South Korea.<sup>37</sup> Service providers in Estonia are also required to assess and manage their information and communications technology (ICT) risks.
- **Sweden** has been developing a long-term plan to enhance its national security. Sweden's aggressive stance towards building a better defensive strategy stems from the fact that its IT infrastructure had been exposed to malicious cybercrime strikes.<sup>38</sup> This was apparent when a recent cyberattack targeted IT systems that public transport authorities relied on. The consequence was significant delays to train schedules and a crash of the Swedish Transport Agency's website.<sup>39</sup> Since then, the Swedish government has focused on public transport systems, telecommunication networks, and powerplants to establish a better defense against future cyber threats. The government also plans on adding to its national defense budget and taking on projects that would encourage the development of smart technologies that would enhance counter strike actions.<sup>40</sup>
- The **UK** has also decided to improve its privacy standards by publishing a minimum cybersecurity standard for all departments.<sup>41</sup> The published document outlines the requirements that must be followed to fulfill obligations set forth in the Security Policy Framework and National Cybersecurity Strategy. Requirements include outlining responsibilities and accountability, training and guidance for senior accountable individuals, testing mechanisms for security purposes, developing an incident response, and strict access control.<sup>42</sup> The strategy behind implementing minimum standards is to increase reliability, minimize downtime, and satisfy compliance requirements.<sup>43</sup>

## 2. Enforcement

A government's ability to deliver timely consequences is essential to deterring malicious cyber activity; this applies to criminals and State actors alike. While solving cybercrime remains challenging, the U.S. and its allies have had increasing success gathering evidence and prosecuting cases, with the assistance and support of other jurisdictions, victims, cybersecurity firms, and outside counsel. Key issues involve obtaining the cooperation of other jurisdictions, acquiring evidence (especially electronically), and creating partnerships with the private sector. Due to the increased volume of cybercrime cases, and lack of proper resources to address them all, agencies are forced to make strategic priority decisions.<sup>44</sup> They may be less likely to pursue cybercrimes occurring at the local level. Those addressing cyber issues often lack necessary resources, expertise, or skills, which can hamper the effective prosecution of crimes.<sup>45</sup>

### Personal Jurisdiction Over Perpetrators

Cybercrime by its nature is not limited to one location; these activities often cross borders which makes it difficult to interrupt and execute enforcement efforts. From an international perspective, this is especially problematic when a perpetrator resides in one country and the victim or target entity is located in another. When jurisdictional issues arise, it is critical to have cooperation in the investigation and prosecution process.<sup>46</sup> The internet is an attractive place to conduct crimes as an individual can remain anonymous and easily take advantage of the internet's financial opportunities. It is not just the issue of whether a country can exercise jurisdiction over an individual or a network, but whether there is an interest in assisting and/or pursuing the same individual(s), and whether the countries can work together to apprehend and prosecute suspects. Without a consensus on applicable law and coordinating strategies, offenders may be able to evade prosecution across international borders by taking advantage of enforcement gaps, or weak or conflicting laws.<sup>47</sup>

#### To Catch a Cyber Thief

Aleksandr Panin, notoriously known as “Harderman” created malware that infected more than 1.4 million computers in the United States and was also responsible for financial theft. Panin is responsible for Spyeye, a software program known as a banking Trojan that collected financial information; thus draining users accounts. To catch Panin, the FBI had to hack into computers and pose as cybercrooks. Panin’s capture shows the elaborate methods and issues U.S. agents had to overcome to catch a cybercriminal. But even when the FBI had enough evidence to link Panin to the conducted crimes, they could not close the case as Russia does not have an extradition treaty with the United States. Luckily, when he arrived in the Dominican Republic, the Dominican police arrested Panin before he could board a plane back to Russia.

U.S. Attorney office, *Cyber Criminal Pleads Guilty to Developing and Distributing Notorious Spyeye Malware*, FBI, (Jan. 28, 2014).

## Collection of Evidence

Another major issue is the collection of evidence needed to prosecute offenders. Many law enforcement agents need specialized training to enable them to adequately collect and analyze digital evidence. Evidence is usually scattered in many different locations as well, making it harder to obtain and preserve evidence in a timely manner. For privacy reasons, service providers are reluctant to provide investigators with their users' information, which can hamper an investigation.<sup>48</sup> There are jurisdictions where investigators and police officials can obtain search warrants or court orders to access information that is otherwise prohibited; however, these techniques are often restricted. Countries have different regulations when it comes to interception. For example, in the UK, the Regulation of Investigatory Powers Act (RIPA) allows law enforcement agencies to conduct intrusive surveillance and monitor communication data.<sup>49</sup> However, evidentiary treatment of data differs in each country, which is why it is important for investigators to understand country frameworks, as well as engage in data mapping. The Budapest Convention helps address some of these issues by providing guidance to participating countries to establish jurisdiction over offenses in unclear situations. If, for example, no matter where a crime is committed, as long as the offender is a national of a signatory state that state is required to exercise criminal jurisdiction over the offense.<sup>50</sup>

## Processes

Even though the United States has implemented some laws to address privacy and cybercrime concerns, enforcing them requires collaboration and sufficient resources. Under Section 5 of the Federal Trade Commission (FTC) Act, the FTC has the power to prohibit unfair and deceptive practices; but when the FTC attempted to establish a data security baseline, companies resisted FTC's efforts to enforce data security practices.<sup>51</sup> Though regulators such as the FTC have attempted to enforce privacy laws, monetary fines have so far provided little incentive for companies to adhere to such policies.

### The Human Element

Officials were able to apprehend infamous drug cartel lord Joaquin "El Chapo" Guzman due to, ironically, the technology he used to spy on his family and workers, and to escape interceptions on his activities. Christian Rodriguez, who had installed his electronic surveillance systems, ended up breaching the security protocols to betray El Chapo. Rodriguez created software that logged the call histories and locations of El Chapo's employees' cell phones, building a network that allowed El Chapo and his associates to communicate in secrecy. While Rodriguez's technological advancements helped El Chapo dodge authorities, it was Rodriguez's betrayal that led to El Chapo's demise.

Sonia Moghe, Meet the IT guy who led authorities to El Chapo's secrets, CNN, (Jan. 10, 2019).

**The Cloud Act**, discussed in the previous section, helps address some enforcement problems. For example, it reduced the burden on the MLAT system, which has been difficult to use due to the huge volume of electronic evidence requests.<sup>52</sup> For a limited amount of time, until the passage of the Cloud Act, the 2016 Microsoft decision<sup>53</sup> hindered officials' ability to obtain electronic data from assisting foreign countries and limited other states' ability to gain evidence from the U.S.<sup>54</sup> The Cloud Act resolved disagreements about the Stored Communications Act (SCA), which resulted from the Microsoft decision. In Microsoft, the Court concluded for the first time that the SCA did not allow the government to require disclosure of data stored

#### Searching Extraterritorially Stored Data

The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Okokrim) was investigating possible computer fraud and searched the office of a private company, Tidal, in relation to the fraud. Tidal itself was not the target of the investigation; the police simply wanted access to information stored by Tidal that could help with their investigation regarding suspected criminal acts. However, Tidal objected to the search, stating that because its data servers were located abroad, the officers were not entitled to a search. Tidal referred to section 199 of the Norwegian Criminal Procedure Act to argue that the right to search is not extended to searches abroad, and that certain provisions were too vague to cover them. The Norwegian Supreme Court disagreed and decided there was no reason to exclude certain devices from being searchable under the provisions. Thus, the Court decided that because there was nothing under the Norwegian law that prevented the search, Okokrim could resume its investigation. This raised questions of confusion with cloud storage practices in Norway.

*Tidal Music AS v. The Public Prosecution Authority*, 19-010640STR-HRET, (March 28, 2019).

abroad with countries subject to the U.S. jurisdiction.<sup>55</sup> Thus, several service providers refused to comply with U.S. court orders to provide data stored abroad, causing difficulty for U.S. authorities to obtain data.<sup>56</sup> The Cloud Act remedied this problem by clarifying the requirement to comply with search warrant requirements under the SCA regardless of whether the communication occurred in or outside the U.S.<sup>57</sup> This does not mean that the Cloud Act expanded U.S. investigative authority, or U.S. jurisdiction to any new parties. The Act merely sought to ensure that companies and service providers hand over data if it is under U.S. jurisdiction, if the entity is an electronic communication provider, and if the entity has possession over the sought material.<sup>58</sup> Essentially, this means that the U.S. must have personal jurisdiction over a company to compel disclosure of data.

## Private Sector

Effective engagement with the private sector is critical, to further investigations, and to engage in education and prevention activities.<sup>59</sup> The Department of Defense Cyber Strategy expressly calls for public-private partnerships.<sup>60</sup> Cyrus Vance, the current District Attorney for New York County, combined forces with other enforcement agencies, the private sector, and research and data gathering entities to create an international cross sectoral effort: The Global Cyber Alliance (GCA).<sup>61</sup> Since its founding in 2015, the Alliance has undertaken projects and activities combat systemic cyber risk in measurable ways, including a recently launched toolkit to providing a small business with easily-deployable resources to mitigate these risks.

However, companies may be reluctant to accept government mandates regarding security measures, as they may be seen as stifling to business operations as well as costly.<sup>62</sup> But instead of seeking to require participation from companies, governments can utilize data to encourage better cooperation. Collected data can show that failure to improve security measures will result in consequences such

as reduced profit, weakened national markets, and growing mistrust from consumers.<sup>63</sup> One example of a successful partnership is a privately managed **Computer Emergency Readiness Team (CERT)** in which personnel from both the government and private sector can exchange knowledge without revealing confidential information.<sup>64</sup> It is imperative that the private sector remain transparent and quick to report timely information. Federal agents can collaborate with those in the private sector to mitigate threats.<sup>65</sup>

In Belize, ABA ROLI ran a public education campaign, developing a resource brochure on financial crimes and distributing over 5,000 copies to banks, credit unions, and other financial institutions.

### 3. Election Security

Election interference in the United States is not a new issue, but greater awareness emerged during and after the 2016 elections. In January 2017, The Office of the Director of National Intelligence published a declassified version of the intelligence community's report on "Assessing Russian Activities and Intentions in Recent U.S. Elections," written by the CIA, FBI, and NSA, concluding with "high confidence" that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election" that included hacking the personal email accounts of Democratic Party officials and political figures.<sup>66</sup> The Mueller investigation confirmed that Russia attempted to undermine the U.S. democratic system.<sup>67</sup> In foreign influence operations, tactics may include targeting voter registration and participation, political organizations, and media outlets.<sup>68</sup> In response to such methods, the Department of Justice has devised strategies to counter foreign operations.<sup>69</sup>

#### Code of Practice Against Disinformation

1. clear policy on identity,
2. tools necessary to aid people in making informed decisions,
3. privacy compliant access to data for researchers, and
4. disclosing rules for issue-based advertising.<sup>1</sup>

Europe Commission, *Code of Practice against disinformation: Commission welcomes the commitment of online platforms ahead of the European elections*, (April 23, 2019).

During the 2016 election process, hackers used social media platforms such as Facebook to promote targeted ads. The groups responsible, who did not initiate mandated filings with the Federal Election Commission, used data to target ads in geographic and interest categories.<sup>70</sup> Russian firms purchased Facebook ads to ferment division between political parties; and an impressive 120 million people saw the ads.<sup>71</sup> Google and Twitter also reported that Russian firms purchased political ads. Data from Facebook ads reveal that states with tight political races, such as Wisconsin and Virginia, were more likely to be targeted.<sup>72</sup>

Targeting was issue-oriented as well as demographic, with Wisconsin voters receiving gun ads 72 percent more often than the national average.<sup>73</sup> Threat researchers from the security firm Invincea discovered that Russian firms employed micro-targeting tools to target defense firms.<sup>74</sup> By using malware-laced advertising, they were able to target individuals through profiles collected from websites. Targeting is based on someone's likes, sharing history, or browsing history.<sup>75</sup>

A National Security Agency (NSA) report stated that hackers from Russia's military intelligence agency sent phishing emails from a fake VR account to 122 states, seeking to trick election officials into downloading malicious software. In Illinois, cyber attackers attempted to delete records in the voter registration database and remained undetected for three days after they accessed publicly available voter files.<sup>76</sup> Luckily, attempts to delete the files were blocked. Since then, Illinois has used some of the 380 million dollars available in election security grants to hire cyber navigators to conduct risk assessments.<sup>77</sup> With the help of the Department of Homeland Security, Illinois performed weekly scans of network traffic to address vulnerabilities, trained officials to recognize malware laced emails, and joined the Elections Infrastructure Information Sharing Analysis Center, which allows state and local officials to exchange threat data practices.<sup>78</sup> Many other states are taking similar initiatives to prepare for the 2020 elections.

## Measures to Counter Election Interference

While the U.S has experienced cyberattacks meant to interfere with the elections, there are established safeguards, including the existing decentralization of election administration. Because there are over 8,000 election jurisdictions, many with differing voting machines and ballots, it is nearly impossible to attack all of the nation's voting machines at the same time.<sup>79</sup> Further, many jurisdictions have supplemented their computerized voting machines with paper ballots, producing a paper trail for verification.<sup>80</sup> Though

### Testing Election Systems

The International Foundation for Electoral Systems (IFES) has developed important strategies for testing election vulnerabilities. Known as Holistic Exposure and Adaptation Testing (HEAT), the process is designed to focus on the virtual exposure that election management bodies (EMB) might encounter when implementing new technology. The HEAT process reflects international practices on data management.

*Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies*, International Foundation for Electoral Systems, (Oct. 17, 2018).

simple, this is one of the better solutions so far. Even though the voting equipment is often not linked to the internet, voting machines are vulnerable to tampering, whether through crashes, stolen memory cards, or erased vote totals.<sup>81</sup>

Some equipment is outdated and relies on old software; these machines are more susceptible to new methods of cyberattacks.<sup>82</sup> Countries such as the Netherlands, Australia, Germany, and Italy have stopped using electronic voting systems, with the Netherlands going so far as to ban them due to security concerns.<sup>83</sup> Germany rendered electronic voting unconstitutional and Ireland has been relying on paper ballots since 2009, due to voters' satisfaction with the system.<sup>84</sup>

## Election Security Worldwide

Cyberattacks on elections are not limited to the U.S. In 2014, cyber attackers interfered with Ukrainian presidential elections by deleting files that made the voting system inoperable just days before the election.<sup>85</sup> In 2018, it was discovered that Twitter accounts were also used to influence the U.S. and UK elections.<sup>86</sup> Investigations reveal that Russia has been attempting to undermine the election system and establish mistrust within the media since at least 2013. The Russian hacker group CyberBerkut has claimed responsibility for interference in Ukrainian elections. Ukraine was

not prepared for such attacks, as its Central Election Commission has lacked technical training and technological vulnerabilities.<sup>87</sup> Russia was also found responsible for the hack against Bulgaria's Central Election Commission in 2015.<sup>88</sup>

### Indonesia in 2019

As Indonesia prepares for its 2019 elections, Arief Budiman, head of the National Election Commission, declared that Chinese and Russian hackers have been attempting to attack Indonesia's voter database to help one of the candidates win. Budiman also stated that voter fraud occurred last year with the creation of 25 million ghost voters. President Joko Widodo runs for re-election against ex-military General Prabowo Subianto, and election watchdogs have noticed a rise in fake news, and false claims meant to discredit Widodo. The election commission has met with social media platforms such as Facebook and Google to ensure that they are not used to manipulate the voting process.

Viriya Singgih, et al, *Indonesia Says Election Under Attack from Chinese, Russian Hackers*, Bloomberg, (March 12, 2019).

With its parliamentary elections in May 2019, the European Commission began focusing on strengthening cybersecurity measures.<sup>89</sup> They recommended that member states set up a national election cooperation network so that authorities can quickly detect and respond to threats. European political parties were urged to be as transparent as possible, including publishing information regarding their advertising campaigns.<sup>90</sup> The Commission proposed a Network of Cybersecurity Competence Centres to coordinate available funding for cybersecurity cooperation. To tackle disinformation issues, the Commission created a self-regulatory Code of Practice for online platforms to ensure more trustworthy campaigns.<sup>91</sup> The advertising industry and online platforms, such as Google and Facebook, are already reporting on their efforts.

The greater impact of election interference on other democratic processes and institutions is also being explored. In its recently released report: "Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System," The Center for Strategic and International Studies states that Russia's disinformation operations go well beyond elections, and are creating vulnerabilities for the justice system, citing the combination of an increased number of individuals on social media, the already existent polarization of discourse, and a general feeling of distrust towards institutions writ large. The report further notes that while the judiciary is more resilient to disinformation than political parties, oftentimes judicial systems are ill equipped to recognize or respond to Russian disinformation.<sup>92</sup>

## 4. Virtual Currencies

Crypto currency is a digital representation of value given through technology that runs on a network of computers. Most are a convertible currency and can be traded back and forth with real currencies. Cryptocurrency coins are disbursed in initial coin offerings (ICO). Bitcoin was the first, and is still the most popular, form of cryptocurrency. The other four largest cryptocurrencies are Ripple, Ethereum, Cash, and EOS.<sup>93</sup> Due to mixed views regarding cryptocurrency, governments around the world have taken different measures and approaches in regulating them. Governments seem to approach the controversial currency in three possible ways: (1) supporting it by developing cryptocurrency industries; (2) banning cryptocurrency or activities supporting it or; (3) seeking to regulate cryptocurrency.<sup>94</sup> Countries such as Malta, Singapore, Switzerland, and Argentina are embracing

cryptocurrency and have created a flourishing environment for ICOs and businesses dealing with cryptocurrency.<sup>95</sup>

In Japan, a world leader in cryptocurrency and its regulations is veering towards linking card payments with digital currencies to regulators, thus encouraging the use of cryptocurrency in the appropriate environment.<sup>96</sup> Japan's view is the opposite to that of China, where the Central Bank formally outlawed ICOs in 2017.<sup>97</sup> The government is also attempting to limit the amount of currency leaving the country, partially due to the US-Sino trade war.<sup>98</sup> But even though the government seeks to discourage Chinese participation in cryptocurrency mining, the country continues to remain a hub for Bitcoin mining and blockchain startups. Like Japan and China, Korea fosters blockchain startups. Initially, South Korea had banned ICOs, but lawmakers did not understand cryptocurrency as well as they do today.<sup>99</sup> Korea may now be reconsidering its barriers to crypto adoption and begin to encourage cryptocurrency development.

### **Using Bitcoin to Counter Sanctions**

Some countries have been using cryptocurrency to evade sanctions and as a terrorist tool. North Korea, for example, has been using cryptocurrency to bypass U.S. sanctions, since digital currencies make it easier to evade such sanctions, and North Korea has been using digital currencies to exploit financial institutions that have a banking relationship with the U.S.<sup>100</sup> Between 2017 and 2018, North Korean hackers stole around 571 million dollars through attacks of five Asia-based cryptocurrency exchanges, which could possibly be used for North Korea's nuclear program.<sup>101</sup> While hackers usually act independently, it is assumed that the North Korean government has been employing hackers through the military to elicit funds for its nuclear program and to counter export restrictions.<sup>102</sup>

When U.S. sanctions took effect against Iran in November, 2018, Iran announced that it would use virtual currencies to avoid sanctions.<sup>103</sup> While the Iranian government had enacted a ban on cryptocurrencies in April 2018, President Trump's sanctions have changed Iran's strategies on cryptocurrency, and the government now promotes its use.<sup>104</sup> Out of economic necessity, Iran seems to be embracing Bitcoin, as the government has recently approved Iranian gold backed currency. Because Iran's currency has decreased significantly, locals and tourists must resort to buying gold or getting Bitcoin.<sup>105</sup> Venezuela is in a similar situation and hopes that its oil backed virtual currency known as Petro will help Venezuela avoid U.S sanctions.<sup>106</sup>

### **Terrorism**

Political extremists who engage in terrorism view digital currencies as an opportunity to conceal the movement of funds, which is what the terrorist organization the Islamic State of Iraq and Syria (ISIS) appeared to do in 2014.<sup>107</sup> Anonymity appeals to extremists and criminals but, contrary to what most believe, virtual currencies are not very useful to terrorist organizations. Big terrorist groups such as ISIS and Al-Qaeda more typically use taxation of businesses and individuals to finance their mission.<sup>108</sup> ISIS attempted to establish financial independence when it created the gold dinar, a physical currency, to supplant the U.S. dollar in its operations. The ISIS dinar ultimately failed.<sup>109</sup> These challenges have not stopped Hamas from creating its own system, a new "wallet" for each transaction to avoid international measures used to interrupt terrorist funding.<sup>110</sup> Hamas launched its website showing how donors can send money using Bitcoin while also protecting their identity. With their piloted program, Hamas was able to receive 3,300 dollars in donations through Bitcoin within a month.<sup>111</sup>

Cash remains more popular than cryptocurrency, but extremists may still use Bitcoin for fundraising purposes. Further, technological advances have made it possible to track Bitcoin.<sup>112</sup> While cryptocurrency is still not feasible for many terrorist groups and organizations, the intelligence community and lawmakers should still be prepared for terrorists taking advantage of this advanced

technology. Previously, Pakistan was against the use of cryptocurrencies, with the country's central bank warning other financial institutions to not provide services in support of virtual currency transactions.<sup>113</sup> But Pakistan decided to introduce the Electronic Money Institutions (EMI) regulations to oversee cryptocurrency.<sup>114</sup> EMIs are non-banking entities that offer cost effective digital payments such as prepaid cards that encourage cashless payments.<sup>115</sup> The regulations will remove barriers for EMIs and provide minimum service standards that will foster secure development for digital payment products.<sup>116</sup>

## Money Laundering

In response to mounting concern over money laundering, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit in 1989 to encourage legal and regulatory standards to address threats to financial systems.<sup>117</sup> The FATF has set recommendations meant to be applied universally, and works to identify vulnerabilities to combat misuse on the financial system.<sup>118</sup> In the past, FATF has issued reports on vulnerabilities regarding anti-money laundering efforts.<sup>119</sup>

An anti-money laundering framework includes laws, regulations and procedures established to combat and prevent the generating of illegal income. These frameworks should require companies and financial institutions to use due diligence procedures when vetting customers and proving that their assets are from a legal source. Illicit traders have used the dark web to create new sources of income.

This was first apparent in the case of the Silk Road darknet market where Bitcoin was the only accepted means of payment, due to its protection of anonymity.<sup>120</sup> Other countries have different approaches in addressing these crimes. South Korea intends to ban the use of anonymous accounts in bitcoin transactions; Singapore restricts activities involving cryptocurrency; and the United States looks to the Commodity Future Trading Commission (CFTC), which retains authority over commodities related to bitcoin.<sup>121</sup>

The National Police Agency in Japan reported that financial transactions involving cryptocurrencies increased ten times over the previous year. Criminals have been using cryptocurrency to purchase child pornography and drugs from underground marketplaces. Japan had introduced regulations in 2017 that make it easier to report laundering cases, which may explain why there were more reported cases in 2018.<sup>122</sup>

Money launderers favor traditional over virtual currencies, since they are untraceable and easy to exchange.

### Simulating Money Laundering

The European Union, in collaboration with the Council of Europe, launched project *iProceeds*, which aims to strengthen the capacity of authorities to prevent money laundering over the internet. COE's *iProceeds* project convened prosecutors, financial intelligence analysts, and cybercrime investigators for a capacity building exercise to address complaints of cybercrime and investigate evidence of cybercrime related to virtual currencies and the Darknet, including through the use of international cooperation channels to trace proceeds.

Council of Europe, *iProceeds: Lasts Series of simulation exercises on cybercrime involving Dark Web concluded in Turkey*, (May 6-9, 2019).

## 5. Trafficking and Crime Convergence

Effectively addressing trafficking activities, whether targeting people, drugs, wildlife, or any number of items, is already complicated, but trafficking through the use of the internet and virtual space creates added challenges. There are two terms often used regarding trafficking online: the deep web and the dark web. The deep web is not accessible to common search engines such as Google, while the dark web is a portion of the deep web that is intentionally hidden from standard web browsers.<sup>123</sup> The origins of the dark web can be traced to the 1990s, when U.S. Naval researchers created technology for communicating anonymously online. At first, this was done to cover up their own activity. But soon the web was recognized as an effective means to conduct illicit activities, especially transnationally, including those focused on child pornography, and human and wildlife trafficking. The dark web is a perfect means for hackers to “meet,” exchange information, and prey on the vulnerable.<sup>124</sup>

### Wildlife Trafficking

Selling animal parts is the fourth biggest illicit industry in the world; after selling drugs, counterfeit goods, and human trafficking.<sup>125</sup> While the dark web provides a place for criminals to engage in crimes, technology and cybersecurity efforts can help target the criminals.<sup>126</sup> The U.S. government has invested in artificial intelligence and cloud computing, but the most helpful tools often come from the private sector, using technological innovations and financial resources to continue combating the wildlife trafficking problem.<sup>127</sup>

Enforcement efforts play a huge part in interrupting and addressing these crimes but traffickers are quick to adapt. For example, seizures may actually cause increases in poaching. Because traffickers already assume that they will lose a percentage of their ivory to law enforcement seizures, they poach even more animals to make up for the losses.<sup>128</sup> The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) initiated a global ban on ivory trade back in 1990, allowing the elephant population to recover.<sup>129</sup> But when a one off auction in 2008 allowed a 15 million dollar sale of ivory to China and Japan, poaching skyrocketed.<sup>130</sup>

#### Dialogues on Illicit Trade

In 2017, ABA ROLI, in coordination with the U.S. and Vietnamese governments, organized the fourth Pathfinder Dialogue on “Combating Corruption and Illicit Trade across the Asia-Pacific Region” during the Asia-Pacific Economic Cooperation (APEC) third Senior Officials Meeting in Ho Chi Minh City, Vietnam. Co-hosted by the Vietnamese and U.S. governments, the conference invited more than 100 participants to share proven methods to combat the harmful role of corruption in illegal logging and wildlife trafficking. Participants represented APEC member economies’ delegations to the APEC Anti-Corruption and Transparency Working Group and the APEC Experts Group on Illegal Logging and Associated Trade, NGOs and international organizations.

Some believe that legalizing trade in some markets will reduce poaching, but these efforts may create a cover for illegal trade and even encourage ivory consumption.<sup>131</sup> Providing solutions to wildlife trafficking is critical, as the profits made from this trade are linked to drug cartels and investments in illegal military supplies.<sup>132</sup> In October 2018, the United Kingdom held its fourth Illegal Wildlife Trade Conference, gathering nongovernmental organizations (NGOs), academics and other key countries.<sup>133</sup> The goal of the conference was to bring together international leadership to stop illegal

wildlife trafficking. The conference brought researchers from around the world to work together in solving the trafficking problem.

### Reducing the Demand for Wildlife Products

In China, it is common to farm wild animals such as tigers and bears. China is known as a largest market for illegal wildlife trading. Tigers are being bred like cattle in order to meet the demands for luxury items such as tiger skin rugs. Bears are also bred for their bile, which is an ingredient used in traditional Chinese medicine. Markets for illegal wildlife products have continued to grow in China, which ends up encouraging poaching in the wild. One way to reduce online demand for wildlife products is having e-commerce sites like Alibaba remove wildlife products from their inventory.

Citation: Simon Worrall, *Inside the Disturbing World of Illegal Wildlife Trade*, National Geographic, (Nov. 9, 2018).

## Human Trafficking

Media platforms such as Facebook and Twitter can serve to facilitate human trafficking, especially through chatrooms and other means to obtain information about victims.<sup>134</sup> Using the same tactics through the surface web, which is accessible through search engines such as Google, traffickers can gain the trust of their victims by accessing their private information. After they form a level of trust with the victim, they may obtain provocative information or photos to blackmail or compromise them.<sup>135</sup> But on the deep web, or the non-searchable part of the web, anonymity is basically guaranteed, offering a perfect harbor for criminal activity.<sup>136</sup>

### Trafficking on the Dark Web

A thirty-year-old Polish man, Lukasz Pawel Herba, claims he is affiliated with a trafficking ring called the Black Death Group. He was attempting to sell a 20-year-old British model, whom he held in captivity for six days. Herba told the model that she would be sold to Arabs, and that he made about 17 million dollars in trafficking a year. Once apprehended, Herba told officials about how he would organize online auctions to sell abducted girls. Herba is an example of the tragedies that occur through advertisements and through the dark web. The Black Death Group website can only be accessed through a specially encrypted invitation with a URL. Interpol, along with the Justice Department, have worked together to shut down websites that promote dark web bazaars. Through undercover operations, officials are able to identify the buyers to prosecute them.

Barbie Latza Nadeau, *Inside Black Death Group, The Dark Web*

Before 2003, about 65% of countries globally did not even have trafficking legislation.<sup>137</sup> By 2008, about 80% of countries had legislation targeting trafficking, a significant improvement. However, traffickers are often located in countries that lack solid frameworks or that have not ratified the Budapest Convention, making it much harder to prosecute traffickers even if identified.<sup>138</sup>

Traffickers also take advantage of company platforms and online sites, advertising victims of sex and labor trafficking across the internet. Institutes that spend time with survivors have experience with

how easy it is to track them using Facebook or the GPS on their phones.<sup>139</sup> Because traffickers are abusing companies' technology to conduct illegal business, companies are more willing to cooperate by providing grants to help anti-trafficking organizations. Google has provided 3 million dollars to fund internet companies such as Salesforce and the Polaris Project that combat human trafficking and slavery; while anti-trafficking organizations continue aid survivors of trafficking.<sup>140</sup>

It is essential that the private and public sectors work together, particularly on enforcement efforts for evidence gathering and analysis purposes. Technology companies have the resources to make image recognition much easier when tracking video footage, for example.<sup>141</sup> While the dark web has been used to facilitate trafficking crimes, new groups such as the Global Commission on Internet Governance are being formed to counter them.<sup>142</sup> Its goal is to provide better human rights protection online and cybercrime cooperation.

## **Drug Trafficking**

Internet-based drug markets reflect the same developments as other illicitly trafficked goods. There has been a trend towards more sophisticated encryption, advertising, increasing availability of high potency products online, and increased movement towards the deep web.<sup>143</sup> Luckily, buyers seem to prefer sellers from their home country, making it easier to prosecute and detect criminals within a country's borders. Adolescents and young adults have increasingly abused prescription opioids and sedatives but only a small percentage purchase prescription drugs online.

Silk Road was one of the largest marketplaces for drug sales online until the FBI shut it down in October 2013.<sup>144</sup> Shutting down Silk Road, however, prompted a more successful site to be created: the SilkRoad 3.0.<sup>145</sup> Crypto markets such as Agora and Evolution became even bigger marketplaces around 2014.<sup>146</sup> Street drugs and prescription medicine were the most popular products being marketed. Online marketplaces are often preferred due to anonymity, opportunity to trade in a low-risk environment, improved product quality, and personal safety.<sup>147</sup> However, on June 2018, the United States Department of Justice sent a message that sellers, not just operators, of the illicit marketplace would be targeted when they charged more than 35 sellers of illegal drug.<sup>148</sup>

There has also been an increase in sales of prescription drugs on the Internet. As of 2016, there were 33,576 active online pharmacies that lacked the appropriate licensing and were providing prescription medication without prescriptions.<sup>149</sup> To establish credentialed pharmacies, the National Association of Boards of Pharmacy created the Verified Internet Pharmacy Practice Sites (VIPPS) program to validate online pharmacies.<sup>150</sup> To receive accreditation, online pharmacies must go through licensing, prescription requirements, and verify the location of business.<sup>151</sup> The European Commission has implemented similar requirements.<sup>152</sup>

## **6. Internet Freedom**

In modern societies, virtual spaces can serve as liberalizing instruments that further broad-based citizen advocacy, democratize public access to information, and improve the accountability and transparency of public agencies and officials. Promoting the advancement of freedom of opinion and expression through virtual spaces, such as social media, can serve as a springboard for the exercise of fundamental human rights, ranging from the right to participate in public affairs to the right to an adequate standard of living. In the United States, the Constitution prioritizes the freedom of speech through its First Amendment, which states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for

a redress of grievances.”<sup>153</sup> The First Amendment is crucial to maintaining a democratic system, as it allows citizens to communicate their opinions freely and without the fear of punishment. Such liberty is limited to harmful speech and lies that can cause harm. However, not every country prioritizes free speech, which can lead to restriction of expression and information.

**The International Covenant on Civil and Political Rights (ICCPR)** sets forth the standard internationally for freedoms of expression.<sup>154</sup> Many jurisdictions, however, struggle with balancing the rights of expression on-line, with the privacy and security interests of their citizens. Brazil, Mexico, Pakistan, and Syria have been criticized for punishing and, on occasion, killing journalists who posted opposing messages online.<sup>155</sup>

In 2017 alone, 14 countries passed legislation to restrict internet use. Fiji, for example, has implemented the Online Safety Act of 2018.<sup>156</sup> The Act imposes a fine of up to 9400 dollars and up to five years in prison if an individual posts an electronic communication that “causes harm” to another.<sup>157</sup> Critics of the Act say it is vague and does not offer protection for legitimate debate and free speech.<sup>158</sup> Fiji has had four coups in its history, and because of the tight control on media, many young Fijians go online looking for alternative sources of information. But in the past several years, social media has acquired a reputation for providing fake news.

In South and Southeast Asia, ABA ROLI helped establish a sustainable network of internet freedom lawyers who can support one another by sharing information and strategy and learn from the experiences of other lawyers in the region.

Fiji is not the only country worried about fake news being shared; in the Philippines, the government increased the penalty for spreading false information.<sup>159</sup> Germany passed a law requiring Facebook and other social media platforms to delete hate speech within 24 hours of it being posted.<sup>160</sup> As a result, allegations of the existence of fake news have enabled lawmakers to push for online censorship, leading the public to question whether this new law is just to regulate people more, or if it truly protects online behavior. Fiji is just one of the countries that has used the excuse of privacy and protection to attempt to chill expression. By analyzing and comparing some of these efforts in Southeast Asian countries below, a better understanding may be gained as to how countries operate to balance these interests.

## India

India’s foundation for freedom of speech and expression is based on Article 19 of the Indian Constitution.<sup>161</sup> Some forms of expression have been addressed through criminal legislation: sedition, defamation, hate speech, morality, obscenity, sexual expression, violations of intellectual property rights, and the use of contempt of court processes. India has some history of criminalizing speech. Examples include arresting group administrators of WhatsApp, and charging Facebook users for defamation and sedition.<sup>162</sup>

One of the most formidable laws regulating cyberspace is the Information Technology Act, which gives the government the power to issue directions for blocking public access of any information through any computer source.<sup>163</sup> Allowing content to be blocked in such a manner violates international standards which require censorship be necessary and implemented in the least restrictive way.<sup>164</sup> Internet shutdowns have been increasingly occurring as well. In 2016, mobile internet services were shut down to prevent cheating in the Revenue Accountants Recruitment Exam.<sup>165</sup> The Supreme Court even maintained that shut downs are sometimes required to maintain law and order.<sup>166</sup>

### India's effort to control content

India's government is proposing to amend the Information Technology Act to trace and access unlawful online content. The amendment would require that encryption be broken to trace its origins, threatening user privacy and free speech. In 2017, the Jammu and Kashmir government blocked 22 social media sites including Facebook and WhatsApp.

*Unshackling Expression: A study on laws criminalizing expression online in Asia*, Association for Progressive Communications, pp. 75, (2017).

## Myanmar

Myanmar has gone from a quasi-military to an attempted civilian-led democratic government. During this transition, it has had setbacks regarding freedom of expression.<sup>167</sup> Under the current government, there have been at least 73 criminal cases initiated regarding online speech, including 30 by private individuals, 12 by the government, and 11 by political parties.<sup>168</sup> Myanmar's 2008 Constitution guarantees freedom of expression and the right to privacy, but it also includes vague limitations. For example, the government reserves the right to restrict freedom of expression based on union security, community peace, and tranquility on public order. The Myanmar government uses provisions of its Electronics Transactions Law and Telecommunications Law to criminalize online speech, and most cases have been initiated under the Telecommunications Law. For example, under the National League for Democracy government, the government has filed about 89 complaints under the Telecommunications Law, arguably for political purposes.<sup>169</sup> In 2017, the government hastily enacted the Law Protecting the Privacy and Security of the Citizen, which protects the privacy of a citizen but still falls short of the standards set by the ICCPR, as it vaguely states that "privacy means the right to freedom of movement, freedom of residence and freedom of speech of a citizen in accordance with the law" and does not explicitly state that privacy is an important right.<sup>170</sup>

## Malaysia

Malaysia has a history of restricting freedom of expression and speech. When civic space started expanding, it was reported that the government and ruling party participated in campaigns through trolls to quiet down dissent. However, the new reform-minded Pakatan Harapan government has made advancing freedom of expression and repealing laws that curtail speech and expression a reform priority. Under Article 10 of the Federal Constitution of Malaysia, freedom of speech and expression is guaranteed but can be restricted by laws relating to the security of the Federation.<sup>171</sup>

Several laws are being used by the state to restrict, censor and punish free speech and expression.<sup>172</sup> While state governments are not given the power to restrict freedom of speech overtly, the option of using Islamic Law can sometimes further these efforts. The Communications and Multimedia Act of 1998 targets the internet and outlines offenses that affect online speech.<sup>173</sup> While it covers all aspects of telecommunications, it could also be interpreted broadly enough to penalize comments made online that could hurt someone's feelings.

## Singapore

Singapore has recently passed the “Protection from Online Falsehoods and Manipulation Bill”, which is aimed to protect society from malicious online falsehoods.<sup>174</sup> The Ministry of Law believes the Bill is necessary to ensure accuracy of information by disrupting the use of false information and, because the Bill does not target opinions and criticisms, it would not be misused for stifling speech.<sup>175</sup> Instead of editing or removing the false information, its intended that facts would be added next to it so that the audience can compare and distinguish between the true and false statements.<sup>176</sup> Those who are found to be malicious actors sharing the false information will be fined up to \$37,000, or five years in prison.<sup>177</sup> The potential abuse lies in the opportunity for any government minister to initiate enforcement of the law if they believe a statement to be false.<sup>178</sup> The law would also cover content produced outside of Singapore. Singapore has had a history of prohibiting speech criticizing the government or policies. The Asia Internet Coalition (AIC), a group that represents Facebook, Google, and LinkedIn are skeptical of the rationale for enacting the bill.<sup>179</sup> AIC is concerned that this bill would give the government full discretion over what is considered true or false and places more restrictions on media censorship.<sup>180</sup>

**Comparison of Penalties<sup>181</sup>**

Category	India	Malaysia	Myanmar
<b>Online Defamation: Penalties</b>	Indian Penal Code, Section 500: Imprisonment for up to two years, or a fine, or both.	Section 233, Communications and Multimedia Act, 1998: “Shall be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offense is continued after conviction”	Section 66(d), Telecommunications Law: Imprisonment for no more than 3 years, OR a fine, or both.
<b>Online Hate Speech: Penalties</b>	Penal Code, 295A: Imprisonment of up to 3 years, a fine, or both	Penal Code, Section 298: Imprisonment of one year, fine, or both.	Penal Code, 295A: Imprisonment of up to two years, fine, or both
<b>Online Offenses</b>	Information technology act: First Conviction gets up to 3 years of imprisonment, and a fine of up to 5 rupees. Second conviction gets up to five years of imprisonment plus a fine of 10 rupees	n/a	Telecommunications Law: Imprisonment for up to 3 years, a fine, or both.

## 7. Incitement

As noted elsewhere in this report, it is difficult to balance constitutionally guaranteed freedoms, such as expression and association, against those risks to safety and security when actions or words are intended to or likely to cause harm or violence. Hate crime legislation is one tool intended to address such situations, but lawmakers and criminal justice actors face challenges in the drafting and implementation of such laws. Ultimately, there is a difficult line to draw when addressing such speech. For instance, when social media platforms such as Facebook have too narrow of a policy, troubling postings might be allowed. If it is too broad, there may be too much confusion and regulation over speech not meant to be harmful. As noted above, Facebook is an example of how the use of hate speech can escalate if social media platforms do not provide adequate oversight over deceptive, unacceptable and possibly dangerous language.

### Social Media as the Problem

Social media providers have algorithms that effectively lure and keep people on social media platforms, especially when certain posts appeal to them.<sup>182</sup> Such algorithms calculate the time a person may spend looking at a post or video, and then recommend similar videos or posts that may be more controversial. Thus, when applied in countries such as Myanmar, where there is already brewing hatred for certain minority or ethnic groups, social media platforms have become a tool for the spreading of misinformation and encouragement to further violence. Another issue is the slow reaction social media providers such as Facebook have had when discovering fake accounts, or troubling content. Brenton Harrison Tarrant, an Australian resident responsible for killing 50 people at two Christchurch Mosques, used Facebook to broadcast his crimes:<sup>183</sup>

#### Livestreaming an Attack

Gunman Brenton Tarrant, an Australian citizen, broadcast his attack on the Al Noor mosque in Christchurch, New Zealand, and though Facebook removed the video 12 minutes after it was posted, it was reposted in other sites such as Twitter. But even before the assault, there were signs of Tarrant's online behavior that social media platforms could have addressed, as Tarrant posted photographs of ammunition and firearms on Twitter and also spent some time tweeting racist videos.

*New Zealand Mosque Shooting suspect ordered to undergo mental health checks, CBS News, (April 5, 2019)*

After Tarrant's broadcasted assault on the mosque, lawmakers have heavily criticized social media platforms for not taking enough action and are calling for more regulation. Videos such as Tarrant's would likely not have surfaced in Germany because of a strict law called the Network Enforcement Act, which fines social media platforms that fail to remove illegal content (such as hate speech or defamation) which may encourage violence.<sup>184</sup>

Germany's stringent laws are likely a result of its own experience with fascism and the horrors of World War II. Unfortunately, companies such as Facebook and YouTube are profit driven and their algorithms have not historically prioritized detection of harmful online behavior. Countries have

varying strategies for regulating social media based on their own history, including in its Constitutional and legal frameworks.

The United States has attempted to avoid too much regulation, for fear of impinging on First Amendment rights, while countries in the EU seem less afraid to impose stronger legislation to force social media to bear more responsibility. After facing much criticism and pressure, Facebook finally changed its policies in 2017. Facebook has divided hate speech attacks into three categories: (1) calls to violence, dehumanizing words, and offensive visual stereotypes; (2) statements of inferiority and; (3) calls for exclusion.<sup>185</sup>

### **The Christchurch Call**

In the wake of the terror attack that was live streamed on Facebook, tech companies and governments made the commitment to tackle extremist content by launching the Christchurch call. New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron launched the action to ensure that effective counter terrorism laws and sufficient measures are being taken to deter extremist content on social media. Tech companies such as Facebook, Google, Twitter, and Microsoft signed the document, and agreed to a nine-point plan. The companies vowed to produce transparency reports on the detection of extremist content, and Facebook in particular stated that they would block anyone from using Facebook Live for 30 days if they share violent content. While this is important response, internet freedom activists note that it may stifle free speech, including postings meant to condemn violence.

*U.S. says it will not join Christchurch call against online terror, BBC News, (May 15, 2019).*

### **Hate Speech Affecting the Muslim Population**

Myanmar military officials have been using Facebook as their platform to encourage violence against the Muslim Rohingya minority group. Myanmar officials posed as popstars, celebrities, and national heroes on Facebook, broadcast their hatred of the minority group and thus prompted a movement of violence against the group.

One frightening example was the fabricated posting of a woman who was raped by two of her Muslim colleagues. The woman who started the rumor later admitted that she was paid to initiate a false police report. Thus far, Facebook has taken down the accounts of the senior officials of the military. By the time Facebook finally acted, about 700,000 Rohingyas had fled from the country to Bangladesh.<sup>186</sup>

Facebook has also deemed four ethnic armies as “dangerous organizations,” including the Arakan army, the Myanmar National Democratic Alliance Army, the Kachin Independence Army and the

### When the State Spreads Rumors

During the Myanmar campaign of 2017, military officials used Facebook to spread rumors that attacks from both Buddhist and Muslim groups were going to occur. Through fake accounts, the military officials continued to warn about jihad attacks and installed fear within both groups about each other. This created an increased and unnecessary reliance on the military's resources and protection.

Paul Mozer, *A Genocide Incited on Facebook, With Posts from Myanmar's Military*, New York Times, (Oct. 15, 2018).

Ta'ang National Liberation Army.<sup>187</sup> Facebook's statement says that groups with a violent mission will be banned, but that is unclear because it does not specify whether it applies to all armies or non-state armed forces.

The use of social media has proved to be critical, however in other circumstances. Journalists and online commentators have benefitted from the use of social media platforms by spreading awareness about such incidents as genocide and political reform movements.

## II. CONCLUSION

Cybersecurity threats are complex, endanger the integrity of the digital world, and are a tool to erode the people's trust in their government and in technological infrastructure. The issues addressed in this paper, and the rule of law strategies identified therein, are grounded in similar strategies implemented for decades in this sector, but virtual spaces create unique challenges. Sound analysis of the breadth of the problem must be a first step, whether designing a program to address conflict related sexual assaults in the DRC or to assist trafficking victims lured via the dark net into lives of sexual slavery in Thailand. The investigations of criminal activity in virtual spaces requires fleet footed reactions and specialized expertise, especially when trying to access and protect electronic evidence that crosses jurisdictions and time zones, some of which is located within countries lacking the will or systems to respond.

Solid constitutional and legislative frameworks, based on international or regional standards, have long served as a critical starting point upon which to build a free society and fair justice system; however, as in the cyber arena, when certain conduct or expression is over-regulated or legislated, or in jurisdictions where there is a misuse of prosecutorial discretion, or the absence of judicial independence, foundational freedoms are jeopardized, if not suppressed. Multi-pronged and holistic efforts must include strategies that combine educational and prevention efforts along with protection and enforcement, and cooperative efforts between law enforcement, civil society groups, the private sector and more. Such strategies are embodied in the efforts of the GCA and other collaborative partnerships.

Governments and organizations should not only collaborate with each other, but also take initiatives that enable flexibility when confronting cybersecurity threats. Such initiatives, as discussed, may incentivize social media platforms and companies to take proactive measures when combatting cybersecurity threats. It is imperative that the evolution and refinement of rule of law strategies stay apace with the quickly changing landscape of virtual threats and remain focused on balancing global security interests with the protection of fundamental rights and freedoms.

## ENDNOTES

- 
- <sup>1</sup> Council of Europe, *Budapest Convention and Related Standards*, (2018).
- <sup>2</sup> United Nations Office on Drugs and Crime, *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*.
- <sup>3</sup> *African Union Convention on Cyber Security and Personal Data Protection*, African Union.
- <sup>4</sup> See Chris Ott, *What You Should Know About the 24/7 Network*, Davis Wright Tremaine LLP, (June 28, 2018).
- <sup>5</sup> European Commission, *What Does the General Data Protection Regulation (GDPR) Cover?*, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en) (last accessed May 17, 2019).
- <sup>6</sup> Stein Schjolberg, *A Geneva Declaration for Cyberspace*, pp. 3, 8, (Jan. 2016).
- <sup>7</sup> Council of Europe, *Peru: accession to Budapest Convention approved by Congress*, (Jan. 30, 2019).
- <sup>8</sup> Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 Inter. J. of Cyber Criminology, pp. 61, (June 2015).
- <sup>9</sup> *Id.*
- <sup>10</sup> Committee Report, American Bar Association, *A Call to Cyber Norms*, ABA, pp. 5 (March 2015).
- <sup>11</sup> See Kristen Eichensehr, *International Agreements-and disagreements-on cybersecurity*, Just Security, (Oct. 24, 2014).
- <sup>12</sup> 18 U.S.C. § 1030 (1984).
- <sup>13</sup> Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, Congressional Research Service, (Oct. 15, 2014).
- <sup>14</sup> 47 U.S.C. § 230 (1934).
- <sup>15</sup> Kathleen Ann Ruane, *How Broad a Shield? A Brief overview of Section 230 of the Communications Decency Act*, Congressional Research Service, (Feb. 21, 2018).
- <sup>16</sup> Jazdia Butler & Greg Nojeim, *Cybersecurity Information Sharing in the "Ominous" Budget Bill*, CDT (Dec. 17, 2015).
- <sup>17</sup> *Id.*
- <sup>18</sup> Dept. of Justice, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the Cloud Act*, pp. 3, (April 2019).
- <sup>19</sup> See generally Dept. of Justice, *supra* note 18.
- <sup>20</sup> *Id.* at 7.
- <sup>21</sup> *Vulnerabilities Equities Policy and Process for the United States Government*, White House, pp. 1 (Nov. 15, 2017).
- <sup>22</sup> *Summary, Dept. of Defense Cyber Strategy*, Dept. of Defense, (2018).
- <sup>23</sup> James E. Baker, *Between Hacks and Hostilities*, ABA Journal, (May 9, 2019).
- <sup>24</sup> Digital and Cyberspace Program, *Reforming the U.S. Approach to Data Protection and Privacy*, Council on Foreign Relations, (Jan. 30, 2018).
- <sup>25</sup> Robert Chesney, *The Cyberspace Solarium Commission: A Timely Proposal*, Lawfare, (June 20, 2018).
- <sup>26</sup> *Id.*
- <sup>27</sup> *Id.*
- <sup>28</sup> Maggie Miller, *Sen King, Rep Gallagher to chair Bipartisan commission to defend US in cyberspace*, The Hill, (May 8, 2019).
- <sup>29</sup> *Id.*
- <sup>30</sup> Jeff John Roberts, *The GDPR is in Effect: Should U.S. Companies be Afraid?*, Fortune, (May 25, 2018).
- <sup>31</sup> *Id.*
- <sup>32</sup> Sarah Jeong, *No One's Ready for GDPR*, The Verge, (May 22, 2018).
- <sup>33</sup> *Id.*
- <sup>34</sup> *Id.*
- <sup>35</sup> *Id.*
- <sup>36</sup> *Id.*
- <sup>37</sup> *Top Ten Countries Best Prepared Against Cyber Attacks*, The Cyber Research Database, <https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/> (last accessed May 17, 2019).
- <sup>38</sup> Gerard O'Dwyer, *Sweden steps up cyber defense measures*, Computer Weekly, (Jan 8, 2018).
- <sup>39</sup> *Id.*

---

<sup>40</sup> Id.

<sup>41</sup> Warwick Ashford, *UK government cybersecurity standard welcome*, Computer Weekly, (June 29, 2018).

<sup>42</sup> Id.

<sup>43</sup> Id.

<sup>44</sup> Brown, *supra* note 8, at 63.

<sup>45</sup> Id. at 65.

<sup>46</sup> Jody R. Westby, *International Guide to Combatting Cybercrime*, American Bar Association, xxvi, (2003).

<sup>47</sup> Brown *supra* note 8, at 62.

<sup>48</sup> Id. at 68.

<sup>49</sup> Id. at 70.

<sup>50</sup> Westby, *supra* note 46, at 65.

<sup>51</sup> Council on Foreign Relations, *supra* note 24.

<sup>52</sup> Dept. of Justice, *supra* note 18.

<sup>53</sup> Appellate Court stated that the Stored Communications Act (SCA) did not require Microsoft to disclose information in its custody, which was stored in Ireland. Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016).

<sup>54</sup> Dept. of Justice, *supra* note 18.

<sup>55</sup> Id. at 7.

<sup>56</sup> Id.

<sup>57</sup> Id.

<sup>58</sup> Matthias Artzt, *How to Comply with both GDPR and the Cloud Act*, International Association of Privacy Professionals, (Jan. 29, 2019).

<sup>59</sup> Chatham House Rule, *supra* note, 10 at 29.

<sup>60</sup> Dept. of Defense Release, DoD Releases 2018 DoD Cyber Strategy and Cyber Posture Review, Chips, (Sept. 19, 2018).

<sup>61</sup> See generally Global Cyber Alliance, <https://www.globalcyberalliance.org/>, (last accessed May 16, 2019).

<sup>62</sup> Chatham House Rule, *supra* note 10, at 31.

<sup>63</sup> Id. at 32.

<sup>64</sup> Id. at 33.

<sup>65</sup> Brian Harrell, *Private Sector is the Key to Success for the Department of Homeland Security*, CSO, (Feb. 1, 2017).

<sup>66</sup> *Background to "Assessing Russian Activities and Intentions in Recent US Elections*, Director of National Intelligence, pp. 1, (Jan. 6, 2017).

<sup>67</sup> Ellen Nakashima, *Mueller Report Highlights scope of election security challenge*, Washington Post, (April 20, 2019).

<sup>68</sup> Office of the Deputy Attorney General, *Report of the Attorney General's Cyber Digital Task Force*, Department of Justice, pp. 3-5, (July 2, 2019).

<sup>69</sup> Id. at 8.

<sup>70</sup> Ellen Smith, *We've Been Hacked-so will the data be weaponized to influence election 2019? Here's what to look for*, The Conversation (Feb. 21, 2019).

<sup>71</sup> Anup Ghosh, *How Elections are Hacked via social media profiling*, CSO (May 31, 2018).

<sup>72</sup> Id.

<sup>73</sup> Id.

<sup>74</sup> Id.

<sup>75</sup> Id.

<sup>76</sup> Lawrence Norden & Ian Vandewalker, *Securing Elections from Foreign Interference*, Brennan Center for Justice, pp. 15, (2017).

<sup>77</sup> Smith, *supra* note 70.

<sup>78</sup> Id.

<sup>79</sup> Norden, *supra* note 76, at 8.

<sup>80</sup> Id.

<sup>81</sup> Id. at 9.

<sup>82</sup> Id.

<sup>83</sup> *Global Election Security*, Secure Our Vote, <https://secureourvote.us/learn-more/global-election-security>, (last accessed May 16, 2019).

- 
- <sup>84</sup> Id.
- <sup>85</sup> Norden, *supra* note 76, at 7.
- <sup>86</sup> House of Commons, *Disinformation and 'fake news': Final Report*, pp. 74, (Feb. 19, 2019).
- <sup>87</sup> Jonas Claes & Jack Stuart, *Protecting Elections from Cyberattacks*, United States Institute of Peace, (April 1, 2019).
- <sup>88</sup> Norden, *supra* note 76, at 7.
- <sup>89</sup> Europe Commission, *State of the Union 2018: Europe Commission proposes measures for securing free and fair European Elections*, (Sept. 12, 2018),
- <sup>90</sup> Id.
- <sup>91</sup> European Commission, *Free and Fair European Elections*, pp. 2, (Sept. 12, 2019).
- <sup>92</sup> Suzanne Spaulding, et al, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System*, Center for Strategic and International Studies, p. 8, (May 1, 2019).
- <sup>93</sup> Rebecca M. Nelson, *International Approaches to Digital Currencies*, Congressional Research Service, pp. 4, (Dec. 19, 2018).
- <sup>94</sup> Id. at 5-7.
- <sup>95</sup> Id. at 5-6.
- <sup>96</sup> Christopher Williams, *East Asia is cryptocurrency frontline as regulation develops in China, Japan, Korea and Taiwan*, Dapp Life, (April 12, 2019).
- <sup>97</sup> Id.
- <sup>98</sup> Id.
- <sup>99</sup> Id.
- <sup>100</sup> Omar Faridi, *\$200 Million: North Korea may be 'Mixing', 'Shifting', Cryptocurrencies to Acquire USD*, Cyber Intelligence Researchers Say, Crypto Globe.
- <sup>101</sup> Rahul Nambiampurath, *North Korea Supposedly Using Cryptocurrency to Fund its Nuclear Program*, Being Crypto (Accessed May 7, 2019), <https://beincrypto.com/north-korea-supposedly-using-cryptocurrency-to-fund-its-nuclear-program/>.
- <sup>102</sup> Tanya Chepkova, *Korea may be a cryptocurrency whale*, Being Crypto, (last accessed May 7, 2019), <https://beincrypto.com/north-korea-may-be-a-cryptocurrency-whale/>.
- <sup>103</sup> Ciphertrace, *Cryptocurrency Anti-Money Laundering Report, 2018*, pp. 13, (Jan. 2019).
- <sup>104</sup> Tom Nyarunda, *Cryptocurrency News: Iran Sees Tourists with Bitcoin as Solution to Sanctions*, Blockchainreporter, (March 23, 2019).
- <sup>105</sup> Id.
- <sup>106</sup> *Ciphertrace, supra* note 103, at 13.
- <sup>107</sup> Tom Keatinge, et al, *Virtual Currencies and Terrorist Financing: assessing the Risks and evaluating responses*, European Parliament, pp. 32, (May 2018).
- <sup>108</sup> Id. at 29.
- <sup>109</sup> Id. at 44.
- <sup>110</sup> *Hamas Develops Bitcoin System to Avoid Terror Funding Sanction*, The Tower, (April 29, 2019).
- <sup>111</sup> Id.
- <sup>112</sup> Samuel Wan, *Homeland Security Bill is Overkill, Bitcoin isn't good for Terrorists*, News BTC, (March 13, 2019).
- <sup>113</sup> Id.
- <sup>114</sup> *Regulations for Electronic Money Institutions Launces in Pakistan*, The Biz Update, (April 1, 2019).
- <sup>115</sup> Id.
- <sup>116</sup> Id.
- <sup>117</sup> FATF, *Who We Are*, <https://www.fatf-gafi.org/about/>.
- <sup>118</sup> Id.
- <sup>119</sup> Robert Chesney, *The Cyberspace Solarium Commission: A Timely Proposal*, Lawfare, (June 20, 2018).
- <sup>120</sup> Andrew Norry, *Bitcoin and Money Laundering: Complete Guide to Worldwide Regulations*, Block Onomi, (July 2, 2018).
- <sup>121</sup> Id.
- <sup>122</sup> AnTy, *Japan's National Police Agency Reports 10x Increase in Crypto Laundering*, Bitcoin Exchange Guide, (Feb. 28, 2019).
- <sup>123</sup> Jane Mounteney, et al, *The Internet and Drug Makers*, European Monitoring Centre for Drugs and Drug Addiction, pp. 5.

- 
- <sup>124</sup> *Internet Organized Crime Threat Assessment*, Europol, pp. 39, (2017).
- <sup>125</sup> *AWF and Irdeto Join Forces to Hunt Down Wildlife Crimes Online*, African Wildlife Foundation, (Dec. 10, 2018).
- <sup>126</sup> *Id.*
- <sup>127</sup> *Criminal Elements: Illegal Wildlife Trafficking, Organized Crime, and National Security*, Wilson Center, (Dec. 6, 2017).
- <sup>128</sup> *Id.*
- <sup>129</sup> *Wild laws: China and its Role in Illicit Wildlife Trade*, Wilson Center, <https://www.wilsoncenter.org/event/wild-laws-china-and-its-role-illicit-wildlife-trade> (last accessed May 17, 2019).
- <sup>130</sup> *Id.*
- <sup>131</sup> *Id.*
- <sup>132</sup> *Id.*
- <sup>133</sup> *Evidence to Action*, Illegal Wildlife Trade, <http://www.illegalwildlifetrade.net/iwt18event/> (last accessed May 17, 2019).
- <sup>134</sup> L.M Rhodes, *Human Trafficking as Cybercrime*, Agora, pp. 24.
- <sup>135</sup> *Id.* at 25.
- <sup>136</sup> *Id.*
- <sup>137</sup> *Global Report on Trafficking in Persons*, United Nations Office on Drugs and Crime, pp. 36, (Feb. 2009).
- <sup>138</sup> Athanassia Sykiotou, *Cybercrime and Human Trafficking*, Vienne Institute for International Dialogue and Cooperation.
- <sup>139</sup> *Human Traffickers Play Catch Up as Criminals go High Tech*, The Guardian, (July 29, 2013).
- <sup>140</sup> *Id.*
- <sup>141</sup> *Supra* note 124, at 40.
- <sup>142</sup> Rhodes *supra* note 134, at 26.
- <sup>143</sup> Mounteney, *supra* note 123, at 8.
- <sup>144</sup> Michael Chertoff, *A public policy perspective of the Dark Web*, J. of Cyber Policy.
- <sup>145</sup> *Id.*
- <sup>146</sup> Mounteney, *supra* note 123, at 5.
- <sup>147</sup> *Id.* at 6.
- <sup>148</sup> Kate Benner & Sheera Frenkel, *Drug Dealers Targeted in Sweep of Illicit Online Marketplaces*, New York Times, (June 26, 2018).
- <sup>149</sup> David S. Festinger, et al, *Use of the Internet to Obtain Drugs without a Prescription Among Treatment Involved Adolescents and Young Adults*, J. Child Adolesc Subst Abuse, (2016).
- <sup>150</sup> *Id.*
- <sup>151</sup> *Id.*
- <sup>152</sup> *Id.*
- <sup>153</sup> U.S. Const. amend. I.
- <sup>154</sup> *Unshackling Expression: A study on laws criminalizing expression online in Asia*, Association for Progressive Communications, pp. 18, (2017).
- <sup>155</sup> Iain Thomson, *Think the US is Alone? 18 countries had their elections hacked last year*, The Register, (Nov. 14, 2017).
- <sup>156</sup> Mong Palatino, *Is Fiji's Online Safety Act a Trojan Horse for Online Censorship*, Advox, (Jan. 22, 2019).
- <sup>157</sup> *Id.*
- <sup>158</sup> *Id.*
- <sup>159</sup> Daniel Malloy, *How the World's Governments Are Fighting Fake News*, Ozy, (Sept. 28, 2017).
- <sup>160</sup> *Id.*
- <sup>161</sup> *Supra* note 154, at 51.
- <sup>162</sup> *Id.* at 75.
- <sup>163</sup> *Id.* at 67.
- <sup>164</sup> *Id.* at 67.
- <sup>165</sup> *Id.* at 74.
- <sup>166</sup> *Id.*

---

<sup>167</sup> *Unshackling Expression: A study on laws criminalizing expression online in Asia*, Association for Progressive Communications, pp. 95, (2017).

<sup>168</sup> Id.

<sup>169</sup> Id.

<sup>170</sup> Id.

<sup>171</sup> Federal Constitution, Art. 10.

<sup>172</sup> *Supra* note 154, at 23.

<sup>173</sup> Id.

<sup>174</sup> Associated Press, *Singapore Just Passed A Controversial Bill Criminalizing Fake News*, Time, (May 9, 2019).

<sup>175</sup> Ministry of Law, Singapore, *New Bill to Protect Society from Online Falsehoods and Malicious Actors*, (April 1, 2019).

<sup>176</sup> Id.

<sup>177</sup> Jon Russell, *Singapore's Proposed 'Fake News' law could stifle free speech*, Tech Crunch, (accessed May 8, 2019).

<sup>178</sup> Id.

<sup>179</sup> Id.

<sup>180</sup> Id.

<sup>181</sup> *Supra* note 154, at 27-32.

<sup>182</sup> Morgan Meaker, *When Social Media Inspires Real Life Violence*, DW, (Nov. 11, 2018).

<sup>183</sup> CBS News, *New Zealand Mosque Shooting suspect ordered to undergo mental health checks*, (April 5, 2019).

<sup>184</sup> Polly Mosendz & Gerrit De Vynck, *Facebook and Google are Guilty of a Failure to Take Ownership*, Bloomberg.

<sup>185</sup> Simon Van Zuylen-Wood, *"Men are Scum": Inside Facebook's War on Hate Speech*, Vanity Fair, (March 2019).

<sup>186</sup> Paul Mozur, *A Genocide Incited on Facebook, with Posts from Myanmar's Military*, The New York Times, (Oct. 15, 2018).

<sup>187</sup> Julia Carrie Wong, *'Overreacting to Failure': Facebook's New Myanmar strategy baffles local activists*, The Guardian, (Feb. 7, 2019).



*Our mission is to promote justice, economic opportunity,  
and human dignity through the rule of law.*

JOIN THE CONVERSATION

**#CyberspaceIRL**



[www.abaruleoflaw.blogspot.com](http://www.abaruleoflaw.blogspot.com)



ABA Rule of Law Initiative



@ABARuleofLaw



@ABARuleofLaw

STAY CONNECTED  
[WWW.abarol.org](http://WWW.abarol.org)