#CyberspaceIRL: Rule of Law Approaches to Virtual Threats

Final Report
American Bar Association Rule of Law Initiative
2019 Conference on Contemporary Rule of Law Issues

May 21, 2019
#Cyberspace IRL: Rule of Law Approaches to Virtual Threats

Final Report

American Bar Association Rule of Law Initiative
2019 Conference on Contemporary Rule of Law Issues

May 21, 2019

The views expressed herein have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the American Bar Association.
Acknowledgements

This report is based on a conference organized by the American Bar Association Rule of Law Initiative (ABA ROLI), and co-sponsored by the United States Institute of Peace, the ABA Standing Committee on Law and National Security, and the ABA Section on Criminal Justice. The conference planning working group consisted of Mary Greer, Tara Mobaraki, Jessie Tannenbaum, Samantha Tu, Shea Wilcox, Greg Taylor, Susan Goldman, and Linda Bishai. Particular thanks go to the ABA ROLI Outreach team: David Dettman, Lorraine Cook, and Jeremy Purcell. Additional — and critical — assistance was provided by members of the ABA ROLI board, especially Judge Margaret McKeown, Judge James E. Baker, and Peter Baugher.

Extensive support was provided by a group of committed volunteers and rapporteurs: Carlin Van Schaik, Diana Thomson, Hayley Rose, Mindie Bernard, Susan Goldman, Shea Wilcox, Claire Duguid, Aruke Masylkanova, Danielle Gray, Becky Greubel, Asmik Arutyunyan, Margaret Wiggins, Dana Lisk, Hanna Jamei, Jill Sandor, Nicole Rodrigues, Hillary Forden, Alyssa Jackson, and Alexandria Farris.

We would also like to thank our co-sponsors at the United States Institute of Peace, the dozens of invited speakers and moderators who participated and lent their expertise to the success of the conference, and the 200 attendees who engaged in a fully day of stimulating discussions. Particular appreciation goes to the keynote speakers: Sujit Raman, Glenn Gerstell, and Judge James E. Baker, and to David Yang, Alberto Mora and Judge Margaret McKeown for their introductory remarks.

This report was prepared by the ABA ROLI Director of Research, Evaluation and Learning, Linda Bishai, with thanks to the conference working group members. Special thanks to Diana Thomson for editing and formatting the notes in preparation for the report.
EXECUTIVE SUMMARY

The American Bar Association Rule of Law Initiative 2019 Conference on Contemporary Rule of Law Issues addressed crimes and threats online and related issues of privacy, freedom of speech, and cybersecurity. As governments and individuals grapple with a rapidly changing landscape of threats and escalating technological capacities, it is critical to include rule of law actors in the conversation about how to address these complex challenges. Legal solutions at the domestic and international levels are key components in protecting the rights and privacy of citizens, preserving democratic institutions, and providing appropriate tools and agile processes to law enforcement responses. On May 21, 2019, more than 200 government officials, law enforcement officers, private sector leaders, non-governmental implementers, academic researchers, media, and activists met to discuss the thorny questions presented by good and bad uses of cyberspace and online technologies. As countries struggle to develop globally applicable legal frameworks for law enforcement and to decide whether a global cybercrime convention is possible or regional standards are a more realistic goal, the conference drew attention to several key challenges, including: election security and attacks on democratic institutions, the balance of internet freedom and personal privacy, trafficking crimes in the digital age, the use and abuse of cryptocurrencies, and confronting online incitement to violence.

Throughout the course of the day, a number of common themes and recommendations emerged. These are summarized and captured at the end of this report. The conference was launched by keynote speaker Sujit Raman, Associate Deputy Attorney General of the United States, describing a new era of great power competition in cyberspace with foreign adversaries weaponizing digital information to undermine democratic values. The best response, he argued, is to require maximum transparency, registration, and disclosure of relationships to foreign governments to enable to public to be fully informed of the source of information. Among the recurring themes conference participants raised was a clear emphasis on the importance of cooperation between law enforcement, legislators, and the private sector to address the challenges of strengthening cybersecurity while protecting constitutional rights and citizen privacy. This also includes building the capacity of legal actors and institutions at national and local levels all around the world to enable informed collaboration and regulation. Additionally, private, public and civil society sectors must work together to improve oversight and management of the media (including social media) to better protect the rights of targeted groups when protected speech verges on incitement.
Participants were quick to stress that cyberspace and online technologies present magnified opportunities both for good and for bad as they provide for connectivity and sharing but also the ability to skirt oversight and regulation and operate outside of the law. One of the more sober observations was on the rapid evolution of cryptocurrencies at the nation state level – providing a challenge to current international financial regulatory institutions that cannot keep up. Additionally, the trend in requiring local data storage by tech companies fractures the internet and creates sovereign pockets operating outside of global norms. As closing speaker, Glenn Gerstell, General Counsel of the National Security Agency, observed, we currently face an unprecedented level of technological change and we must deal with its effect on our laws and our privacy. There is no time to waste in developing and promoting global norms for cyberspace.
INTRODUCTION

Conference Theme and Goals

The hyper advancement of information sharing and associated technologies in recent decades has provided unprecedented opportunities for enhanced connections and communications across the world, but unparalleled challenges have accompanied these advancements. In few areas are those challenges more apparent than when addressing crimes with potentially global breadth and import, such as cybercrimes. The sophisticated techniques used by individuals or groups to impact, influence, disrupt, or disconnect, acting alone on a laptop, or within advanced networks, require fleet-footed, proactive and constantly updated counters to such activity, whether initiated by or against governments, businesses or individuals. Enforcement efforts alone are insufficient to address these challenges: targeted and holistic strategies encompassing cross jurisdictional cooperation between government and non-government institutions and actors, the private sector, and other key players must be prioritized as well, both globally and locally.

Effectively addressing these challenges requires consistent adherence to international conventions, protocols, and best practices, as well as a synchronistic confluence of criminal and regulatory reform. The only binding international instrument on this issue, the Convention on Cybercrime of the Council of Europe (known as the Budapest Convention), with its protocols and guidance notes, serves as a guideline 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 drafting efforts address the access to and use of evidence in the Cloud as well as providing much needed protocols for emergency mutual assistance. The United Nations Convention against Transnational Organized Crime (also known as UNTOC) and its protocols provide mechanisms for international cooperation to combat transnational organized crimes, including cybercrimes. Many countries, especially signatories to both the Budapest and the UNTOC Conventions, have enacted legislation and procedures addressing these crimes.

To contribute to the international discussion and response to the complex issues surrounding cybercrimes, the American Bar Association Rule of Law Initiative (ABA ROLI) devoted its 2019 Annual Conference on Contemporary Rule of Law Issues to identifying rule of law strategies to more effectively address cybercrimes. The day-long conference was intended to address not only the complexity of the issues, but also identifying the breadth of actors outside the enforcement arena, especially from the private sector, who by necessity must be part of devising and implementing effective strategies or
solutions. Break-out sessions examined legislative frameworks and conventions and addressed enforcement challenges including with convergent crimes like money laundering and trafficking, as well as case studies and targeted discussions diving more deeply into alarming related consequences of cybercrimes such as election security and the erosion of trust in democratic institutions.

Conference Participants and Stakeholders

“#Cyberspace IRL: Rule of Law Approaches to Virtual Threats” was convened by ABA ROLI in partnership with the United States Institute of Peace and co-sponsored by the ABA Standing Committee on Law and National Security and the ABA Section on Criminal Justice. The conference convened 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 aimed at exchanging lessons learned and articulating a shared agenda for addressing the rule of law dimensions of cybercrime.

Conference Outcomes

In preparation for the conference, ABA ROLI prepared a background paper as part of its Rule of Law Issues paper series, surveying academic and policy literature on rule of law strategies in addressing cybercrimes, highlighting ABA ROLI’s work, lessons learned about potential policy responses, and supporting technical assistance implementers in highlighting legal responses proven to be effective, and developing strategies that can shape rule of law approaches. Key highlights and recommendations by the participants will be listed at the end of this report.
Sujit Raman, Associate Deputy Attorney General in the U.S. Department of Justice, opened the conference with framing remarks about the ungoverned and challenging nature of cyberspace. No topic could be more timely than bolstering the rule of law in cyberspace. Adversaries and competitors are using cyber capabilities to seek political, economic, and military advantage. Threats are not limited to state actors but include organized crime and terrorist networks seeking to access and steal information, trade secrets, political information, and access to infrastructure. Cyberspace is the modern wild west, where people act in ungoverned physical spaces. Raman’s address touched on three main ideas. First, we have moved into a new era of great power competition. Governments are using the internet to control their own populations and leveraging its unregulated nature to undermine American hegemony. Second, law is critically important in regulating the cyber arena. However, while international law continues to develop in this sphere, the focus of the Department of Justice will be on how U.S. law can support cyber norms. Third, foreign adversaries are weaponizing digital information to undermine democratic values. The important point is that under the Constitution, the U.S. is not powerless to confront deceptive misuse of cyberspace.

Raman explained that structurally, cyberspace is composed of three layers: physical, logical, and persona. The physical layer consists of hardware and infrastructure. The persona layer is comprised of the digital representations that humans create in order to participate in the online world, such as email addresses and social media profiles. The middle layer is the logical, “code,” where data exists and that links networks together. This is the internet’s nervous system. To promote rapid growth and connectivity, the openness of the logical layer was prioritized, and security wasn’t. Every computer was assumed to be trustworthy, but it wasn’t long before this openness was used for ill purposes. Authoritarian nations have used this feature to censor data within their borders: for example, China’s great firewall and Russia’s strategy of being unplugged from international cyberspace. Thus, the growth of the internet solidified authoritarian regimes’ hold over their citizens. Raman argued that the growth of the internet has fundamentally reordered international relations. The internet is being used to intrude into confidential affairs and access information. Attackers carefully operate below the threshold of the use of force so as to not elicit responses from other nations. Cyberthreats used to be about espionage, but the situation has worsened since 2013 when network attacks began to be
distributed across private companies within the U.S. This has had a continual, cumulative, and strategic impact through the erosion of political, economic, and military assets. Therefore, great power competition has revived and transitioned to cyber space. As a priority action to counter this threat, law enforcement plays an important role. At the Department of Justice (DOJ), this means protecting national security by preventing, targeting, and disrupting transnational crime syndicates, and especially those operating in virtual spaces.

DOJ implements a variety of strategies, including intelligence collection and diplomacy, and especially enforcement -- publicly charging foreign nations and state actors for cybercrimes -- because the charging of state actors is critical. Nation states are engaging in behavior that departs from international norms of state behavior, norms that benefit all nations, and the DOJ response reflects the severity of the threat. These actions are not legitimate statecraft, they are crimes without justification in international relations. The increased number of indictments reflect an increased ability to attribute these crimes to individuals and states and demonstrates how law enforcement and intelligence agencies can work to counter cybercrime. This approach of cooperation was forged in the context of countering terrorism, where a combined approach is required.

Raman then explained the six principles guiding DOJ’s response. The first is the duty to enforce the law and protect people. Where there is a severe violation of privacy rights, DOJ has an obligation to work to ensure business can be conducted without threats to its virtual security. The second is that attribution is the key to deterrence. Attribution means that there can be consequences, the prospect of criminal indictment can deter criminal actors and provides a framework for engagement. The third is using the power of the filing of criminal indictments to expose state conduct through the introduction of facts and application of law during open and transparent criminal justice processes. The fourth is that unsealed indictments increase transparency. There is a limit to transparency with sensitive information, but there are things that can be exposed to the international community and educate to the public. The fifth is that DOJ’s investigative response is part of a wider civil, diplomatic, economic and military strategy and toolkit - for example, restricting financial transactions, offensive cyber interactions, blocking assets, access to banking, and trade sanctions. The sixth is using public law to protect private citizens, establishing a framework for public private cooperation to ensure cybersecurity. DOJ cannot prosecute its
way out of the issue, but to dismiss the role of law enforcement in the fight against cyber threats is to diminish the nation’s powerful commitment to the rule of law within and beyond its borders.

Finally, how can we deal with one of the latest and potentially most destabilizing manifestations of great power competition in cyberspace, namely, adversarial use of information to subvert democratic institutions, specifically elections? Foreign actors are spreading divisive information, fabricating news stories, and reaching an unprecedented number of people without setting foot on U.S. soil. They have sought to weaponize free speech and individual liberty. Foreign attempts have taken many forms from the covert funding of newspapers to fake government communications. The traditional response has required transparency such as registering as foreign actors, filing reports, and disclosing their relationship to foreign governments on any materials. This ensures that the public and lawmakers know the source of the information that may be trying to influence laws.

In defending our elections are we limited to domestic election disclosure laws and are we limited to disclosing such conduct only after it occurs? Or can we take covert preventive action to keep foreign cyber-enabled campaigns from influencing our elections? The answer is yes. If persons are interfering in our elections, the government can act to prevent this conduct in a manner that is consistent with the First Amendment. Non-U.S. persons are not protected under the First Amendment, nor are external state actors. A more complex question becomes, would such hypothetical action outside of the U.S. violate the First Amendment rights of U.S. citizens? It is established U.S. law that as consumers, citizens have the right to receive information, independent of any right the distributor of this information has and therefore preventive actions could implicate the rights of citizens. This is not an issue if U.S. action works on information that is disseminated covertly. Supreme Court precedent presumes that those with a right to receive information can evaluate the source of that information, but there is no right to receive covert information. As he discussed constitutional considerations, Raman emphasized that his thinking is tentative and focused on two assumptions – that the foreign action is covert and that U.S. responses are for the purpose of securing elections. Raman closed by emphasizing that how we respond to these challenges now will have far-reaching consequences. He quoted from U.S. Supreme Court Justice Robert H. Jackson in the wake of the Second World War. Jackson wrote of a “heavy responsibility to see that our behavior during this unsettled period will direct the world’s thought toward a firmer enforcement of the laws.” We too must act to ensure that in these unsettled times the world is directed to a “firmer enforcement of the laws.”
The Council of Europe’s Convention on Cybercrime, also known as the Budapest Convention, is the only binding legal instrument promoting coordinated, international regulation of cyberspace. It has been ratified by 47 countries and influences national cybercrime legislation around the world. Yet, major players in this realm (e.g., Brazil, China, India, and Russia) have not signed on to it. This panel explored opportunities and initiatives to expand this and other frameworks, addressing critical questions on protection of privacy and speech rights, and the role of the private sector in cyberspace regulation.

Moderator Rob Leventhal, of the Office of Anticrime Programs at the Department of State, opened this session, remarking that cybercrime is the quintessential international crime, and international assistance is paramount. Laws don’t have to be identical, but some similarities are necessary because it makes it easier to cooperate. International assistance mechanisms range from bilateral agreements to informal networks. Policy in this realm tends to reflect liberal democracy regarding free speech and multiple stakeholders, etc., but some countries stress a top down authoritarian approach that may threaten human rights and liberal values.

Rodolfo Orjales, a consultant with the Council of Europe, and former Senior Trial Attorney with Department of Justice in the Computer Crime and Intellectual Property Section, began with the history of laws governing cyberspace. Laws dealing with these issues are not up to date, some date to 1955, and they cannot deal with modern issues. The idea behind the drafting of the Budapest Convention was that cybercrime is an international problem and cooperation is necessary to fight it. After a decade of negotiations, the convention was open for signatures in 2001. The Convention defines common terms like “computer”, “server”, and “data”; and includes substantive provisions for standardized crime and procedural provisions for responding collectively in the digital world. Orjales explained that it doesn’t matter which legal system a country has, parties to the Convention need some way to expeditiously preserve data and electronic evidence because everything can be deleted at the push of the button. The Convention calls for a mechanism to preserve data without a court order. The Convention affirms the need for balance between maintaining privacy for citizens and protecting security.

In describing the benefits of the Convention, Orjales gave the example of Blue Whale, an online platform in which disenfranchised teens connected online, mutilated themselves, and in some cases committed suicide. Argentine authorities found out about Blue Whale because participants were using Facebook messenger. They tried to
reach Facebook to get subscriber information under an emergency exception, which allows service providers to provide necessary information when there is a life-threatening situation or death is imminent. When Facebook refused to provide the information, Argentine authorities contacted DOJ. DOJ recognized this as an emergency and called Facebook; they still refused. Orjales argued with Facebook that if DOJ could not assist in this case and people wanted to know why, and it became public that Facebook refused to help, it would have an impact on their shares. DOJ got the records in 2 hours. Based on the information Facebook provided, Orjales found the precise house and gave the information to the Argentine authorities. Six lives were saved.

Kenn Kern, from the New York County District Attorney’s Office, described how the DA’s office is at heart a local prosecutor’s office. It handles 60,000 to 100,000 cases a year, and Kern described it as “the emergency room of society.” But the DA’s office is also an international office because of its Wall Street and technological jurisdiction. The office can look through local and international lenses, and what goes through the NY DA’s office affects both local and international citizens. The DA’s office has personnel in London, Paris, and Israel because these are central locations in combating cybercrime. Kern said that it is always better to prevent a crime than to try to only address it through criminal processes. Time is very important in cyber cases because criminals act with speed and law enforcement cannot keep up. He talked about the nonprofit Global Cyber Alliance (GCA). The New York County DA’s office, the London Police, and Center for Internet Security came together to form the GCA to figure out how to prevent cybercrimes across borders. The GCA is made up of 250 private and public partners across eighteen sectors and twenty-eight countries. Sectors include government, healthcare, finance, energy, transport, media, tech, insurance, and defense manufacturing.

When the GCA was first formed, the unanimous answer to the question of what it should focus on was phishing. Phishing is the leading cause of economic losses related to data breaches today. Large institutions can combat cybercrime, but a lot of small and medium businesses cannot, and these make up the majority of New York City’s businesses, so the DA’s office had to figure out how to help them combat cyber-attacks. Kern described DMARC, where one can download tools to help prevent attacks on email, and Quad9 which is a toolkit for small businesses. Improved cybersecurity trainings for what cities and businesses should do if crimes occur are very promising.

Mary Greer of ABA ROLI said that we need to identify what rule of law strategies are most effective in cyberspace. Programs designed after personal experience are the most effective and assessing has to happen all along the way. Assessing involves asking if people are saf-
er and if prosecutors are implementing enforcement mechanisms, among other things. Greer then discussed the breadth and depth of rule of law strategies. The breadth involves dealing with multiple justice actors, not just enforcement and Ministry of Justice actors. There is also the need to include institutions like ombudsmen, anti-corruption agencies, regulators, and consortia, both regionally and globally. Strategic depth involves individuals, business owners, and multiple stakeholders, and training is important not just for the high judicial actor, but also for the conservation officer in Tanzania and the police officer in Tbilisi. Many of the spaces involved are tightly governed, so finding common ground with countries and governments who keep a close grip on internet freedom is important.

Greer then discussed some practical concerns for enforcement. She said that prosecutors often lack the evidence from a legal standpoint to charge or convict people of the crimes they committed, so there need to be other enforcement measures. If prosecutors lack of proper evidence of a cybercrime, they may have to do something creative, like going after an individual’s professional license or permit to conduct business. Greer emphasized the intersection of human rights and labor and the need to bring in the private sector to work with public agencies. Lawyers have gotten better at assisting victims and representing defendants being prosecuted by governmental overreaching, and the public and private sectors and civil society have been brought together to deal with these spaces in sensitive countries.

During the Q&A session, panelists discussed how private entities can filter traffic and how the legal frameworks affect and help them. Facebook alone, with two billion users, can make global cyber policy change. The DA’s office never misses opportunity to take advantage of private sector good will, and deals with Facebook frequently. Rule of law strategies, public information and education campaigns are acutely needed for the private sector.

Another question probed the issue of why countries do or do not sign on to the Budapest Convention. Countries that are not signatories generally fall into one of three categories. The first are less developed countries that do not rely on ecommerce. These countries usually wake up after someone very important becomes the victim of attack. For example, the Dominican Republic mobilized when its president was the victim of a cyber-attack and has now become a cybersecurity leader in the region. The next category includes the more restrictive countries, like China and Russia. They remain concerned about maintaining sovereignty and they do not want judges in France to issue orders for Chinese internet records. The reality is that Convention signatories may never be able to work together with such countries. The third group are countries like Brazil that come up with different reasons not to sign, such as having issues with the articles regarding intellectual property. Brazil is promoting the negotia-

“Many countries that are not signatories to the Budapest Convention still base their cybercrime laws on the Convention.”
tion of a new treaty. They want to know why they were not involved from the beginning and since they were not, they want a new treaty. However, the Budapest Convention took a decade to negotiate, so the U.S. suggests that Brazil join the Budapest Convention and work on new terms. Many countries that are not signatories to the Budapest Convention still base their cybercrime laws on the Convention.

When a question came up about encryption, Kern said the keys are to investigate, exonerate, and prosecute. Before 2014, law enforcement could get a warrant from a judge to get into a smartphone to find information on crimes. In 2014, Apple changed its operating system, which proved a huge challenge for the DA’s office. Now most phones cannot be cracked even if a warrant is issued, so there is legal but not physical authority. There are practical implications; in about 9% of homicides or attempted murder, child sex abuse, trafficking, assault, cybercrime or ID theft, devices might provide evidence of strong corroboration from the victim. This is a societal issue--balancing public safety with privacy. The DA’s office is stuck because it cannot get to evidence. There is a white paper on this subject on the website (manhattanda.org).

Leventhal summed up the main themes of the panel. The first is the need for adequate legal frameworks as crime has evolved and common elements help cooperation. Second is the importance of capacity building, and of thinking not just federal to federal, but subnational to subnational. Third is the theme of constraints and innovative approaches to fighting cybercrime, and fourth is the balance between privacy and security in combatting cybercrime.

“Now most phones cannot be cracked even if a warrant is issued, so there is legal but not physical authority.”
“Perceptions around cyber-attacks are becoming just as pernicious as the attacks themselves, so trust in the system is being eroded.”

**BREAKOUT SESSIONS:**

**Election Security and the Erosion of Trust in Democratic Institutions**

Foreign influence operations and even individual hackers target elections to undermine confidence in democracy. This panel examined the threats and challenges that cyber operations pose to electoral processes and democratic institutions more broadly. Panelists outlined measures to prevent and mitigate attacks and drew specific examples from the recent elections in Indonesia and Ukraine, among other cases.

Moderator Jonas Claes, a senior program officer at the U.S. Institute of Peace, began by saying that it is important to think about different phases of the election cycle that pose different cybersecurity risks; elections are not just an event but a long process that presents varying sets of risks and opportunities throughout. Elections are made up of pre-elections, which involve voter registration systems, and a campaign phase, which are more vulnerable to cyber-attacks. There is also election day, which involves the voting process itself and interference with the mechanisms of voting. The last part is the post-election which involves the vote processing systems and interference in vote counting to decrease confidence in electoral outcome. Cyberattacks may not only change results but can reduce trust in the system itself and in some cases when there is a controversial outcome can translate into physical violence.

Katherine Ellena, Legal Advisor at the International Foundation for Electoral Systems (IFES), spoke about the challenges faced by election management bodies and explained some common cybersecurity misconceptions. The first misconception is that elections face the same problems as cybersecurity challenges in other areas. Electoral security requires thinking critically about when technology is introduced and how to protect users and their information. In Indonesia, the types of threats and attacks on elections are diversifying, with 2,000-3,000 potential incursions per month. In Ukraine, legal frameworks were not keeping up and did not even mention the internet in 2004, despite it being ubiquitous. Elections rely on public trust, and there must be transparency so an election result can be verifiable and trusted, and so these systems must provide maximum transparency while protecting security. Perceptions around cyberattacks are becoming just as pernicious as the attacks themselves, so trust in the system is being eroded.

The second misconception is that it’s primarily a problem for countries with a high level of digital use, which is not true. Incursions into electronic results transmissions are not the only thing we have to be worried about. Perceptions of attacks can be just as damaging as actual incursions. Website attacks affecting public information about elections are common even in systems where elections are strongly paper-based. The third misconception is that cybersecurity is just for cyber experts themselves.
The 2014 presidential election in Kenya was annulled due to perceived failures in the electoral system, despite an incredibly highly prescribed technology framework in the law. IFES pays close attention to inauthentic actors who commonly interfere to create or amplify disinformation. IFES sees the actions of inauthentic actors as a chain or process, made up of inauthentic action, which is either alone or coordinated, and may or may not involve a foreign government; artificial amplification; interpreters; and risk.

Harvey Rishikof, former senior policy advisor to the director of national counterintelligence at the Office of the Director of National Intelligence, discussed Russian efforts to undermine trust in electoral systems. The national security community has concurred that this issue is a priority. Russian President Vladimir Putin has said that Russian malign attacks were motivated at least partially as retaliation for the U.S. government’s incursions in Russia. In authoritarian regimes, election outcomes are predetermined so the process is not very important, and elections are a light form of legitimization, but for democracy, elections are central and can often be unpredictable, so a trusted process is critical.

The U.S. disadvantage in the face of soft attacks is complicated by unregulated markets, commitments to free speech, and the free exchange of ideas -- strengths that have now been made into weaknesses. The U.S. is loath to regulate content, especially political speech. Social media legally is seen not as a publisher of information but as a platform, which makes the legal landscape very complicated. The constitutional tendency is to deal with problematic speech by adding more speech. U.S. adversaries have replaced this by adding fake speech, which makes it very difficult for receivers to determine signal and legitimacy. The U.S. needs to decide what its basic value system will be in dealing with these challenges.

Rishikof discussed persistent engagement and the need to create a new strategic framework for constructing cyber norms. New norms about interference in other country’s elections need to emerge as well as standards for attribution and the need to develop an enforcement mechanism that will be a sufficient deterrent for our adversaries. Finally, there is the important question of how the U.S. can both regulate and respect the First Amendment.

Saleela Salhuddin, Cybersecurity Policy Lead at Facebook, discussed how Facebook analyzes security threats to keep the Facebook platform safe. Election security and integrity is a priority and more has been invested by Facebook in election security than went into preparation for its initial public offering. Lessons were learned from the 2016 election, resulting in the development of policy regarding Global Coordinated Inauthentic Behavior (CIB). CIB is a network of pages, accounts, or groups acting together in a coordinated manner, but misleading others about who or what they are, in order to achieve a strategic goal.
The first phase of the misinformation process is the point of origin, which involves fake accounts, created by bots or inauthentic users. The creation phase can come from off-platform sources, websites or groups that are not originated on Facebook that often center on wedge issues in society, which cause debates that foment discourse and unrest. The second stage is seeding, where the inauthentic begins morphing with the authentic. Real communities start to take the inauthentic information and spread it. The third is amplification. This is the critical stage, and perception vs. reality is impacted by who amplifies the message and the resulting impression of its legitimacy. It could be journalists who want a headline or think they are covering a real story, political actors, sympathetic communities and off-platform actors.

Salhuddin then discussed the ways in which Facebook controls CIB while trying not to limit users’ rights. The first is technical interception, which involves technical behavioral signals that undermine the persona presented online, for example someone saying they are a mother from the Midwest, but their account was created from a computer in China. The second aims to create a space where real activism, political speech, and political discourse by an authentic actor with any opinion can thrive, but to draw the line at inauthenticity. Facebook has seen success during the iterative process and over the past several elections.

The threat landscape requires partnerships with security researchers, vendors, civil society, and other governments, because not all countries have the same intelligence and rule of law landscape as the U.S. Resilience and knowledge are built through exposure and hopefully the effect from these threats can be dampened. Google, Microsoft, and Twitter have all been excellent corporate partners in this fight.

During the Q&A session, panelists discussed how there are multiple types of bots, such as those that automate ecommerce and digital democracy. Facebook has invested significant resources in bot detection for fake accounts, removing more than 2 billion bots pre-upload in 2018. Detection systems are strong and 99.6% of those accounts are proactively detected by Facebook. Users can also flag fake accounts, and once reviewed, they can be removed. If content violates Facebook content standards or suppresses votes, it will be taken down. Flagged content that says it might violate standards will be sent to a nonpolitical and verified fact checker.

Rishikof postulated that if the public thinks the process is somehow manipulated and Facebook is forced to take something down, this creates a perception of de-legitimacy around the process. So even being successful in these efforts communicates to the audience that there is interference and ends up undermining public trust in discourse. He then explained how cyberattacks happen in the first
place. Actors find cracks in the system and sow the seed of distortion, with the goal of building audiences. He discussed credibility, saying that there must be alternative independent authenticators that a rational third party would agree do not have bias in this authentication process. Public education is also a method of addressing this.

Ellena said that we are in a period of international legal experimentation on how to respond to these threats. There is anti-bot legislation coming out in Europe; content regulation under debate in Germany, Italy, and India; and legislation around modes of communication. There is legislation about advertising and extending campaign silence periods; for example, Indonesia banned foreign IPs on election day and many days after that. Because such legislation can be used to stifle free speech it requires real attention. Some of this experimentation is concerning, but regulation over different parts of the chain is necessary. Domestically, commentators are saying the decentralized nature of our election systems is a strength, which is not true. The decentralization means that hackers do not have to change all of the results, just the right results, and so they just need a strategy to influence a very small number of voters in a very strategic area. Information/influence campaigns and inauthentic disinformation can be even more influential in a decentralized system. There is also a lack of clarity of judicial recourse in a decentralized system.

Addressing a question about whether artificial intelligence could make the challenges harder, Salhuddin said that Facebook is thinking about issues from a policy perspective and hoped that her presence at the conference demonstrates how committed Facebook is to consultation and addressing these issues.

Rishikof emphasized the deep commitment to privacy in U.S. democracy. If there is a commitment to privacy, metadata can be encrypted; but the economic model of social media is to know who a person is, and to use their data for a market purpose. Individuals protecting and owning their own privacy is the real tension with the social media model. The U.S. system struggles to balance individuality, privacy, and transparency.

Ellena said that traditional transparency measures help preserve public trust, and gave an example of Indonesia, where all paper result sheets were posted online for each district and civil society organizations crowd-sourced results sheets and showed that the election result matched that of the traditional methods. Investing in cybersecurity infrastructures to protect from foreign incursions has been shown to be effective once you get the structure in place. Countries need to share their approaches to regulation, whether or not it is working, and develop mechanisms to address this and learn from each other to produce feasible solutions.

“...decentralization means that hackers do not have to change all of the results, just the right results, and so they just need a strategy to influence a very small number of voters in a very strategic area.”
Cyber incitement is based on the idea that there is a connection between online speech and real-world violence. The panelists in this session, moderated by Lata Nott, Executive Director of the First Amendment Center, examined the role of social media and other online platforms in inciting, or amplifying calls for violence.

Richard Wilson, Professor of Law and Anthropology at the University of Connecticut School of Law began the session. To counter hate speech and regulate content in the global context, tech and social media companies like Facebook set community guidelines to establish rules about the kinds of speech and content that can be shared on their platforms, and employ a diverse group of monitors who can review content in the language in which it was shared. Facebook’s community guidelines establish tiers to measure the severity of a violation, and identify protected groups, or categories of individuals who may be targets of hate speech because of their gender, sexual orientation, race, ethnicity, etc.

Describing the case study of Guatemala, Wilson explained that the tools that tech and social media companies use to remove hate speech or content that violates community guidelines are designed to address individual posts, or individual user accounts. When the offending speech or content comes from prominent state actors, including military leaders, political leaders, official statements by government institutions, or state press releases, as has been the case in Guatemala, these tools are not equipped to remove the content or the source. State actor speech in Guatemala targeted human rights defenders (HRDs) in particular, and Facebook does not categorize HRDs as a protected group. This meant that calls for violence and dehumanizing speech against HRDs were allowed to be shared widely in Guatemala, and at the same time there were violent physical attacks against HRDs. How can oversight bodies (meaning state governments, international organizations, watchdog organizations, etc.) measure the extent to which online speech may have caused or contributed to physical violence? And how can the law be used to protect targets of cyber incitement and pursue accountability for inciters?

One finding from Wilson’s study was that the language used online to target HRDs was “coded,” often using slang that was culturally or politically specific to Guatemala. This meant that Facebook monitors who were not native Guatemalans would not have the contextual knowledge to flag the language’s offensive, dangerous, or violent nature. Among the recommendations of the study: monitors should be natives of the countries or contexts being monitored to ensure they...
are able to identify the cultural nuances of the speech or content and evaluate it in context against the community guidelines. Additionally, the proliferation of fake accounts or bots amplified the speech and made it difficult for Facebook monitors to contain the spread of content once it was obtained by a series of bots.

Criminal law requires a clear cause and effect scenario to hold individuals accountable, and this does not fit the nature of cyber incitement. Criminal law will likely fail to address the need to connect cyber incitement with real-world crimes, despite an understanding that dehumanizing speech can contribute to increased tolerance for violence against the dehumanized group. Wilson recommended that it is up to lawmakers and stakeholders in government and civil society to pursue rule of law approaches to accountability for cyber incitement.

Cyber incitement and online speech that dehumanized HRDs in Guatemala may have contributed to an increased tolerance for violence against HRDs. The real or perceived authority of the speaker or source of the speech, and the political context, can play a role in the public response to that speech. Tech companies should work with their monitoring teams to consider contextual triggers, such as elections and political processes, and the authority of the speaker, such as state actors, when evaluating what content to remove.

Stephanie Kleine-Ahlbrandt, a member of the Panel of Experts Established pursuant to UNSCR 1874, spoke next. She said that authoritarian governments have a range of tools at their disposal to suppress freedom of expression and deny privacy to groups they identify as dangerous or undesirable. Free speech is often only granted to select groups and is subject to regulations by company norms and legal boundaries that are rarely transparent. When the speech is coded, or contains contextually-specific nuance, it can exist under the radar of tech company algorithms. This was the case for speech against the Rohingya in Myanmar, and South Sudanese HRDs. In Myanmar, the hashtag #rohingyasarebengalis, which arguably called for bringing harm upon the Rohingya because it was inferring they were not Burmese, flew under the radar because it was coded. Algorithms require the humans designing them to agree on what constitutes hate speech; what rules should apply; who should be protected; and how to enforce, review, and update on a constant basis without bias. Hate speech is probably too fast and too flexible for algorithms to keep up.

Kleine-Ahlbrandt recommended that to protect the rights of targeted groups, private, public, and civil society sectors must work together to improve oversight and management of the media and data collection. In the private sector, individuals’ data is shared between actors rapidly, secretly, and for a profit. The public sector must have the capacity and the tools to identify what constitutes a violation of individual rights to privacy and hold violators accountable within a justice system.
Decision-making should be de-centralized. Platform users do not currently have systematic opportunities to influence the enforcement or creation of the rules. Users can flag a post for review or suggest that a post violates community guidelines. They have no influence in the decision-making process of what the community guidelines deem acceptable or unacceptable, and they have no power to appeal the decision to remove or tolerate particular posts, speech, language, or terminology. International human rights standards should inform community guidelines, and ideally be the basis for those standards. Principles on business and human rights could give private sector companies the guidelines, authority, and justification they need to support their decisions to remove certain speech or content.

There should be more transparency in the way companies make decisions to address content. Companies can elaborate and publish clear reasoning for their decisions, which would provide clarity to users, and help to establish precedents. Public decision making should be accompanied by clarity in the inputs to algorithms and artificial intelligence tools that flag content. Businesses should have mandatory oversight boards, or “social media councils” that are independent enough to investigate and monitor case decisions. Finally, companies need to retain removed content in an organized way, such as a database. The removed content could support legal processes, including war crimes trials. Governments should invest in regulating and monitoring tech companies, to enforce transparency and promote greater public understanding of the rules and the right to freedom of expression. There are lessons to be learned from a few European countries, including Germany, on this front.

During Q&A, the panelists discussed the effect of regulating speech on mainstream platforms, and whether that would just move hate speech to marginalized spaces that are harder to monitor. They agreed that removing content and publicizing that similar content will be removed may have the effect of pushing speech to social margins, such as websites run by extremist groups and white supremacists in the U.S. An alternative to that is to combat individual hate speech with “counter-speech,” which has proven effective. However, when the hate speech is authored by mainstream actors, such as state actors, as in Guatemala and Myanmar, we know that a much more mainstream approach is needed. The approach must be widespread, visible, and systematic to show that the mainstream actors are promoting extremist or unacceptable speech.

The speakers were asked whether they had immediate guidance for HRDs based on these findings. The answer was that HRDs should be trained to respond to trolls and identify red flags. Incitements to violence and harassment should always be reported, preferably to a number of actors in the public, private, and civil society sectors. States should be encouraged to exercise their responsibilities to protect HRDs and other vulnerable or targeted groups.
State capacity to criminally prosecute online abuses is essential to deterring malicious cyber activity, but difficulties in attribution of attacks, collection of evidence, and lack of legal precedent in cyberspace has made successful prosecution challenging. During this session, panelists outlined lessons that the U.S. and its allies have drawn from their work in this area and discussed how shifting international norms can promote or detract from their efforts.

Steven Kelly, Chief of Cyber Policy at the FBI Cyber Division, led the panel discussion with Luke Dembosky, a partner at Debevoise & Plimpton; Michael J. Stawasz, the Deputy Chief for Computer Crime at the U.S. Department of Justice, Computer Crime and Intellectual Property Section; Sean Newell, the Deputy Chief for Cyber with the U.S. Department of Justice, Counterintelligence and Export Control Section; and William Lyne, a Liaison Officer with the National Crime Agency at British Embassy to the U.S.

Kelly described how society has become desensitized to data breaches and election hacks, and that the fact that those who commit cybercrimes are rarely in the same country as the victim makes these crimes unique. Nations are bulking up their defenses and increasingly working together, and there is a fundamental responsibility for states to fight cybercrime in their territories. Stawasz replied that there are limiting factors to cybercrime enforcement such as the scope of the computer crime section at DOJ being limited to attacks and intrusions for criminal purposes, and not every cyber breach is in this category. Terrorism and state actors are covered by another division.

Dembosky works with victim organizations in combating crime. Not all victims have the same level of experience in working with enforcement. Big financial sector actors have more experience and know how to cooperate with each other and with the government, but even they still face issues. Cyber breaches are an existential issue for many of the firm’s clients. For an entity, if the whole network is hit, they might be offline for days, and this could be the end their business. For individuals, a cyber breach could easily be the end of a job or career. In a world where the “bad guys” are changing, relationships are a constant formula for success in combatting cybercrime. It’s important to figure out how to find common ground, and how different players can trust each other, taking the time to explain processes to companies that could be victims. The issue is when and not if their company will be attacked — if a company has information worth accessing, then it is a target.

“'The issue is when and not if their company will be attacked — if a company has information worth accessing, then it is a target.'
Newell said that DOJ is making news by taking action against criminals acting on behalf of governments. At some point, leadership said the usual criminal investigation approach is no longer working in the cyber realm, because things are happening at cyber speed. As enforcement agencies are watching and surveilling, cyber criminals are sucking away millions of dollars. Enforcement agencies need to arrest actors working for state governments from safe havens. Cyber criminals used to be relatively anonymous, but this is decreasingly the case. Cyber criminals now have to think about whether they are as anonymous as they used to be, whether committing these crimes will affect their future if they want to travel or go clean and enter the legitimate business world, and this has a deterrent effect on these individuals.

Lyne heads the British embassy's cyber liaison team in the U.S. He said that the state of play on cyber-crime is that cyber criminals no longer have to be tech savvy due to new trends, lowering for barrier to entry in committing cyber-crime due to a proliferation of sophisticated techniques. A cybercriminal can now just pay people to put clean bitcoin into his or her account. Cyber networks are connected, and criminals collaborate better than those trying to combat cybercrime. Government agencies either deal with the crime aspect or the national security aspect, when the issue is really both -- as in the case of criminal actors who have the support or backing of a nation state. The panel discussed the ease of committing cybercrimes. Carding forums used to be closed societies. Now those who want to commit cybercrimes don’t have to be technologically savvy to hide themselves online and find people to help them. Networks that sell cybercrimes as services are available to the mass market and the barrier to entry has been lowered almost to zero. One no longer needs to have technological capability to buy a malware package, spam the malware, and hit antivirus vendors. If he or she wants to monetize access, they can pay someone to do that also. A good example is ransomware, which is almost a perfect crime. Cash out used to be a big issue for criminals, and a muling network was needed. Now, they just have to drop ransomware and wait to be paid in Bitcoin.

In terms of how to be prepared for cyberattacks, panelists advised businesses to retain specialized counsel in before anything happens. If a company announces its breach at 10 AM, it’s sued by 4 PM, and if a company doesn’t have attorney privilege in place, it is in trouble. High speed investigations within companies are important, as is a new breed of attorneys to do these investigations. Companies need to design an internal system for rapid investigation for cybercrimes. Cybercrime.gov contains information on how to prepare for a cyber-attack. But the best advice is to build relationships in advance, and also working with law enforcement is key. Though it can be difficult for an entity that has just been attacked to want to do so because they have just lost a lot of data and don’t want to share it with anyone else.

“Cyber criminals now have to think about whether they are as anonymous as they used to be, whether committing these crimes will affect their future...”
Attribution has become harder and takes longer to figure out, and there is a question of whether an actor is going to be subject to the criminal process, the national security process or both. It is now harder to find out who is behind an attack. It was already hard to track criminal activity with proxies but there was still a money trail, and now we don’t have money or an electronic trail. When you have mass market ways to anonymously transfer currency and new crimes like ransomware, investigation becomes harder, but crimes are still being solved. In the last two weeks one of the largest services that was referring people to the dark web to buy illegal narcotics was brought down. Cyber criminals now are not just being prosecuted in the U.S., there has also been success with deterrent value in Moldova, Ukraine, and Bulgaria. Because of capacity building, these countries can now do this on their own.

The panel discussed a question from the audience about deterring cybercrimes in the first place. Stawasz said that law enforcement has to solve more of these crimes and explained length of punishments isn’t as important as the fact that there will be punishment, though it is easy and cost effective for Congress to lengthen sentences. He stated that we also need more specialized investigators with increased pay. Citizens should report cybercrime efforts to the cybercrime center at the FBI.

There was also a discussion about ransomware, specifically the ransomware attacks that caused the cities of Atlanta and Baltimore shut down. The Department of Homeland Security and the FBI have put out ransomware advice, and the FBI is working with cities to help them deal with the attacks. The ability to restore from backups is very important in helping attacked entities get back online.

“When you have mass market ways to anonymously transfer currency and new crimes like ransomware, investigation becomes harder, but crimes are still being solved.”
Blockchain-based digital currencies like Bitcoin are ‘blocks’ of recorded transactions that are stored, or ‘chained’ in peer-to-peer computer networks. These virtual currencies have the potential to expand access to capital, crack down on fraud, and reduce transaction costs. Without transparency and regulation, however, they create new pathways for scams, money laundering, terrorist financing, sanctions evasion, and other illegal activities. This panel considered how stakeholders can balance challenges to the rule of law and the legitimate growth of virtual currencies, such as Bitcoin, Ethereum, Zcash, and Monero. Panelists offered insights on how illicit use of virtual currencies can be prevented, detected, and stopped.

Adam Zarazinski, CEO at Inca Digital Securities, moderated the discussion with Elisabeth Poteat, an attorney with the Department of Justice National Security Division; Michael Sachs, Chief of the New York County District Attorney’s Office Investigative Division; and Yaya J. Fanusie, a Fellow at the Foundation for Defense of Democracies. Zarazinski introduced cryptocurrency. Bitcoin is the world’s first decentralized virtual currency. Blockchain is a distributed ledger where people can add things to the bottom, but not change it, and everyone can see it. With Bitcoin, one can hold and transfer money without a bank or any other third parties involved. It’s revolutionary, and presents challenges, especially to banks, and challenges to the rule of law. People can use digital assets to buy drugs and guns, evade sanctions, and fund terrorists. U.S. law enforcement and regulatory agencies are trying to catch up but also have a light touch.

Poteat said that terrorists do use digital assets to fund operations. There are glossy websites for crowd funding terrorists that feature a fighter with a perfect beard and a price for each item they need, including underwear and socks. Cryptocurrency can also be used for travel for people overseas. Generally, material support involves things such as travel for people who want to join terrorist organizations, as well as clothes and technology. Potential funders are targeted over social media. Once a potential funder is reached, communication moves to an encrypted form of communication such as WhatsApp. An advantage to cryptocurrency is that it is outside the regular banking system, with no government backing the currency, and is therefore not subject to anti-laundering rules. An advantage particular to the Middle East is that cryptocurrency allows banking institutions restricted by U.S. sanctions to side-step the restrictions. Fanusie said that using cryptocurrency to purchase supplies must be thought of as retail that accesses the same services as anyone else who wants to get into crypto currency. The concern isn’t if they are successful all the time, but how they work around the problems.
The bottom line is that these campaigners are adapting, and that’s the thing to worry about.

In describing the different kinds of cryptocurrency, panelists explained that there are two kinds of virtual currency. Some are more easily accepted in retail settings or converted into cash in exchanges and can include both legitimate and illegitimate exchanges. Enhanced anonymity currencies are harder to trace. To overcome this, we must rely on traditional law enforcement techniques and on clustering to develop attribution in cryptocurrency cases. Since someone is always having something delivered to an address, search warrants can be obtained. Warrants can also be served on a money service business like an exchange.

Digital currency is only worth something if it can be traded for money or a good or service, so law enforcement looks for those points where the trade can be seen. Pressure points for law enforcement are exchanges where cash is taken and exchanged for digital currency. If such a company is set up in the U.S., it has to comply with certain rules according to the Financial Crimes Enforcement Network (FinCEN). However, if a company is set up in Russia, where there is not as much oversight, it’s harder for law enforcement to get information. There are physical Bitcoin kiosks where currency can be traded for Bitcoin or vice versa. These are often used for narcotics transactions. In one criminal case, investigators were doing surveillance on ATMs and identified individuals and found out that they were selling Xanax pills that were made in a garage. This was all being sold through the dark web with digital currency. It was doing the surveillance and seeing what people were at the ATMs that led to the arrests. Ultimately, it comes down to attribution; we have to be able to identify people or it’s hard to prosecute.

Fanusie described trying to find out how to get Bitcoin in Washington, DC. He took his interns to a Bitcoin ATM and bought about $20 worth of bitcoin. They verified a phone number, but a burner phone could have been used to do so. An ATM allows a user to set up a bitcoin wallet with another exchange. He discovered that it would be very difficult to be totally anonymous. There was a camera above the ATM, so law enforcement would be able to pull video from the ATM camera and do surveillance. If a person wanted to fund terrorists, he or she would have to use another currency or go in person.

“An advantage to cryptocurrency is that it is outside the regular banking system, with no government backing the currency, and is therefore not subject to anti-laundering rules.”

There is a lot of hype about Bitcoin and sanctions. Sanctions evasion is a big business, and cryptocurrency is not by itself enough to evade sanctions. In the short term, we can look at how bad guys are using cryptocurrency; in the medium term, we should look into how priva-
cy currencies are used; and in the long term, we will look at states that are creating their own cryptocurrencies. Even in Iran, which is trying to create its own cryptocurrency, this is a long-term project. But we need to figure out how to keep up and not wake up in 2025 when Russia has its own cryptocurrency and China joins them, and then they’re outside the banking system.

It is also possible that overregulation of cryptocurrency in the U.S. could potentially cause us to lose out on new currency and all the good things it can bring. Weaponization of the U.S. dollar has consequences, virtual currencies may end up linking to something else in the future. Iran, North Korea and eight other nations have tried to develop national currencies to undermine the dollar and efforts to bring them into international financial norms. None have succeeded, but no doubt that they will eventually, especially in places where thinking is more long term. If the U.S. wants to maintain the primacy of the dollar, it needs to carefully think about how it can regulate cryptocurrency, noting that there are well over 1000 cryptocurrencies out there already. There are many good uses of block chain outside of digital currency, and there are other digital currencies that don’t rely on block chain.

During Q&A, panelists discussed the regulatory role of the International Monetary Fund if cryptocurrencies become more prevalent. The Financial Action Task Force (FATF), which sets standards for anti-money laundering and terrorist financing around the world, says each country has to regulate their virtual assets in the same way that they regulate Western Union wire transfers. There will likely be some problems similar to those that already exist involving jurisdictions and variances in their abilities to regulate. But there is an effort to bring countries on board with the same standards.

There are a number of states that have attempted to regulate cryptocurrencies and FinCEN has issued a lot of guidance in this area. The New York State Department of Financial Services issues a bit license for exchanges and keeps certain records about transactions and who uses cryptocurrency. There aren’t any criminal penalties associated with the license, so if a company is ethical, it’s fine since they are licensed. But there are companies that are not getting the license and are not keeping those records. FinCEN has said that digital currency should be treated as currency. New York has not taken that step yet, so it is difficult to charge unlicensed exchanges.

“One of things that most people don’t know about buying digital currency is that there is no way to reverse the transaction because it is not backed by anything.”

One of things that most people don’t know about buying digital currency is that there is no way to reverse the transaction because it is not backed by anything. If a buyer doesn’t receive the good that he or she purchased, there is no way to reverse it. Because Bitcoin uses blockchain, it can be followed to the end, but sellers can use individual wallets for each transaction and that makes it harder to trace.
In recent years there have been high-profile database breaches and news stories about the sharing, selling, and invasive use of personal, online data. There is also heightened awareness of online propaganda and foreign influence campaigns, and repressive regimes’ expansive use of surveillance technologies and repression of online speech rights. These issues have brought internet freedom and privacy protections to the fore of international debate. This panel focused on strategies for protecting internet users’ rights and promoting safe and smart use of cyberspace.

Heather West, Senior Policy Manager at Mozilla, led the panel discussion which included Andrea Little Limbago, Chief Social Scientist of Virtru Bill Marczak, Research Fellow at Citizen Lab and a Postdoctoral Researcher at UC Berkeley, and Robyn Greene, Privacy Policy Manager at Facebook

Limbago described her work on how data privacy and encryption technologies fit into global trends from a global studies perspective. Over the last eight years, internet freedom has been on the decline due to a variety of tools that authoritarian governments are using, but the general goal is to tighten controls over user data and create a “hegemony of communication.” Many countries are putting laws in place requiring local data storage, and of these, some even require government access to that data upon request. This has led to issues with Apple storing some data and encryption keys in China, as well as the recent Facebook manifesto stating that they will not adhere to these laws. This is not just a concern with China and Russia, it’s also a concern with non-state actors and other countries such as Vietnam and Thailand. As this trend spreads, it leads to the “Balkanization of the internet” or the “splinternet.” This means that instead of one global internet, we’re seeing it break apart into “cyber sovereignty” internets across the globe. The most extreme example is the “Great Firewall” of China, but Russia has recently passed a law attempting to cut off access to the rest of the globe. Venezuela is also considering similar legislation.

Unfortunately, there is a vacuum in the space where we would expect to see democracies pushing back. Cyber norms have fallen apart at the government level. Some progress was made with the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), but this also fell apart. Corporations and tech giants are trying to fill this space and create appropriate norms to preserve security and privacy. We should not be naive to the current threat landscape, but we also need to be aspirational and create the internet that we want and make technology much more usable and accessible. The U.S. has left a vacuum in these efforts. California is
coming out with its own data security law, and some states are following this lead, but it is overall a piecemeal issue. What we really need is a data privacy law at the federal level.

Marczak spoke about Citizen Lab’s work looking at commercial spyware -- companies selling products to law enforcement or intelligence agencies to hack into computers or phones of certain targets. Law enforcement often faces the problem that even with a warrant they cannot access encrypted data on phones and computers. These spyware/surveillance companies propose a law enforcement solution by bypassing encryption. The way this typically works is that the target will receive an email with a malicious link or attachment, which they will then open. Once they do so, it will infect their device, leaving it open to surveillance, including listening to or reading encrypted calls, encrypted messages, and the ability to turn on cameras and microphones.

Marczak noted that with these spyware companies, it’s important to keep in mind that it is a much higher level of surveillance than a wiretap, because it can be constantly collecting data and accessing all of the data stored on the phone (contacts, emails, apps with location services). Although these companies present themselves as solutions for law-abiding governments and organizations to defend against criminals and particularly against terrorists, many repressive governments are also interested in this technology and these tools as well. Some examples include Saudi Arabia, the United Arab Emirates, and countries that define terrorism to include criticizing the government.

People often ask how Citizen Lab knows so much about this spyware, a product that we imagine would be private and used only in the shadows. The whole enterprise is dependent upon the people who are targeted not realizing that a message is malicious. If they do realize it, they can send the message to Citizen Lab, Human Rights Watch, Amnesty International, the Electronic Frontier Foundation (EFF), or any other actors working in this space, to analyze what they were sent. For example, an activist in the UAE received a link from an unknown number that said something about “new secrets about torture in the UAE.” They were suspicious and sent it to Citizen Lab, who was able to see the spyware and find the bug in Apple’s software that it was utilizing. They then sent this information to Apple, who then patched the bug. This process of reporting suspicious contacts is essential because it is a way for organizations to pressure the spyware companies. Once this news is public, other consumers will be concerned that the product will no longer work for them because the bug is fixed.

“Although these companies present themselves as solutions for law-abiding governments and organizations to defend against criminals and particularly against terrorists, many repressive governments are also interested in this technology...”
In general, these spyware companies have two markets, “legitimate players,” which include law enforcement agencies and governments with strong human rights records; and abusive or reckless customers, such as the UAE, Saudi Arabia, and Mexico, who use the spyware to target civil society organizations (CSOs). Citizen Lab takes advantage of the companies’ need for the legitimate market by ensuring that when spyware targets CSOs they find it and locate the bug, and it will then get patched, which ruins the product for all users. Ideally, this sends the message that if you target CSOs, your product will be damaged or disclosed, which will then damage your reputation. This is a last resort regulation.

Greene spoke on public safety issues and how Facebook engages with law enforcement on access issues. The focus is always on the individual. To ensure that Facebook can fulfill its mission to help people build communities, share, organize, build businesses, etc., it needs to be sure that it is keeping users safe. At times, this puts Facebook in the uncomfortable position of having to work with law enforcement while simultaneously pushing back against them, often even the same unit of law enforcement. This overarching goal has led Facebook to announce that it will not store data locally in any country that has a bad track record of using citizens’ data maliciously, and countries where it isn’t confident it can keep the users’ data safe.

Facebook is incorporated in the U.S. and Ireland. Law enforcement from the U.S. needs to go through the U.S. judicial process and obtain a warrant for data from Facebook. Law enforcement from EU countries needs to go through the Irish legal process to obtain user data. Non-EU and non-U.S. law enforcement need to go through the mutual legal assistance treaty (MLAT) process with the U.S., which involves requesting a warrant based on probable cause and working with DOJ. After it goes through the legal process, Facebook scrutinizes the request, and decides if it can be applied based on the following criteria: Is it lawful? Is it appropriately scoped? Is it appropriate in purpose? Is the country making the request itself in compliance with International Human Rights Law? If it is not, Facebook will push back on the request by either refusing to comply, working with law enforcement to revise the scope, or taking the request to court. In the case of imminent loss of life, they try to hand off the specific information as quickly as possible to assist law enforcement.

Greene said that Facebook is currently looking for ways to change how it responds to cross-border data requests. As encryption use increases and as data is de-territorialized, questions about jurisdiction become very pressing. The MLAT process in the U.S. requires that foreign governments that are seeking users’ content get warrants based on probable cause. This is very difficult if, as a foreign regime, you do not have the legal concept of probable cause. On average, it can take about a year to respond to a single request, which undermines public safety by impeding serious investigations into legit-
imative crimes. Facebook is encouraging alternative mechanisms for access, such as the recently passed U.S. Cloud Act. This allows governments that meet human rights standards to enter into executive agreements with the U.S. and then directly ask providers for data. Citizen Lab wants to find ways to make it easier for people to access their own data to help an investigation. Many countries have data retention requirements, and it would be great if there were more individual control so that the target of an attack could access their web history and take it to a research groups for investigation.

When asked what they would identify as the top sources for developing norms in this space, panelists advised looking to the UN GGE and its process, and also note some of the collective action problems they ran into as something to avoid as we move forward. The UN GGE looked at “low hanging fruit” for what cyber norms could be (such as not interfering in cyber emergency response efforts, not attacking critical infrastructure in peace time). The U.S.-China Cyber Agreement in 2015 was ostensibly not to allow commercial corporate theft by a government to help their own commercial enterprises. That norm has been broken. However, after the U.S. and China made this agreement, so did China and Australia, and China and Canada, so at least it set a baseline. Additionally, some corporations are involved, doing things like the Paris call, which is an integration of tech corporations and governments from over 100 countries who signed to try to rejuvenate efforts towards creating cyber norms. French President Macron introduced it in November, but the U.S. didn’t sign on. There was The Charter of Trust initiated by Siemens, which is on the corporate level. Microsoft came out with a Tech Accord. There is also talk about the need for a cyber Geneva Convention.

“Ideally, this sends the message that if you target CSOs, your product will be damaged or disclosed, which will then damage your reputation.”
Governments, NGOs, the private sector, and even private citizens around the globe are coordinating and collaborating to halt illegal trafficking, yet effective routes managed by transnational criminal groups or opportunistic actors continue to transfer humans and cargo within and beyond country lines. This panel addressed the convergence of digital, underground economies, and illicit marketplaces for human beings, wildlife, and illegal narcotics. Panelists presented on cases relevant to their respective backgrounds, their use of innovative technologies to combat trafficking, and reported on promising interdisciplinary partnerships for halting these crimes.

Jessie Tannenbaum, Legal Advisor with the ABA ROLI Research, Evaluation, and Learning Office, moderated the panel, which included Danielle Kessler, Senior Policy and Outreach Manager with the International Fund for Animal Welfare; Evan Ratliff, journalist and author of The Mastermind: Drugs, Empire, Murder, Betrayal; and Robert E. Bornstein, Assistant Special Agent in Charge with the Criminal Division of Branch 1 of the FBI’s Washington Field Office.

Bornstein explained that his work with the FBI (which plays a major role in prosecuting child, sex, and labor trafficking) focuses on the violent crime program, particularly overseeing gang violence, violent crime, and trafficking squads in the Washington Field Office. He described three examples of recent trafficking cases involving cyber space. The first was about two rappers who funded their careers by recruiting three child sex workers and pimping them out in Virginia, DC, Maryland, and Georgia. They were convicted in January 2018 and sentenced to 26 years in prison. Trafficking is a $150 billion industry as of 2017 and it is rising. Minors have more independence now, open access to communication devices and the internet, and these things increase their risk of being targeted.

The second example was a man who operated a prostitution ring with his girlfriend out of their home in Virginia. The girls he recruited were underage and were recruited through social media. The man has been sentenced to 30 years, his girlfriend will serve 10 years, and they have been ordered to repay the victims the money they earned while trafficked.

The third case involved a 15-year-old girl who met up with a man from the internet and disappeared. The man had reached out to her over social media, flew from Estonia to pick the girl up in Prince William County, Virginia, and kidnapped her. The man spoofed his IP addresses, so police thought he was in Tampa, Florida, and even raided a home in Tampa where they thought he was hiding. After working with law enforcement partners in Estonia, the American police were able to get the man’s banking info, and determined that he used an
Uber while in the U.S. The police talked to the Uber driver and then tracked the man from there.

The lesson from these cases is that trafficking is not just an international issue, we have to look in our own communities. In the past, we had gatekeepers, such as house phones, that provided a barrier between strangers and children. Traditional law enforcement methods of solving crimes are now being hindered by technology. We don’t have the tools or the legislation to penetrate these anti-encryption environments.

Evan Ratliff spent 5 years reporting on the case of Paul Le Roux, one of the biggest cyber criminals in the world. He recently published a book, The Mastermind: Drugs, Empire, Murder, Betrayal. Paul Le Roux was a self-taught programmer who wrote TrueCrypt, one of the most famous encryption software programs before big companies like Apple and Samsung started creating encryption themselves. He started an online pharmaceutical company based in the Philippines and created hundreds of websites where any customer could fill out a survey of their symptoms and purchase painkillers via credit card. Prescriptions were sent to pharmacies all over the United States.

Le Roux was operating a drug sales distribution network making about $250 million a year. He then got involved in arms trafficking, selling arms to Iran, and recruiting Israeli, American, and South African ex-mercenary to be hitmen to enforce his deals around the world. Le Roux’s operation ran from 2004-2012. The DEA spent five years trying to catch him. Le Roux had bribed high-level officials in the Philippines and had connections in the U.S. embassy and other embassies, so it was extremely difficult to get to him. The DEA eventually lured Le Roux to Brazil and set up a sting operation. When he was caught, he agreed to provide information, particularly on the ex-mercenaries. Three of his hitmen were just sentenced life to prison. Le Roux is still in custody waiting for his sentence. This story touches on every aspect of internet crime, and how criminals such as Le Roux are able to avoid law enforcement and operate globally.

Danielle Kessler said that wildlife cybercrime refers only to the illegal wildlife trade. The Convention on International Trade in Endangered Species (the CITES treaty) lists species and their various levels of protection. Appendix 1 has the highest protection level (a ban on sales), while Appendix 2 allows for legal and sustainable trade (with the right documents). Wildlife trade moved online for the same reasons as any other trade. The internet is available 365 days a year, increases global access to markets, and is always open. Usually trade is happening on open source platforms because it is so extensive. There is a little bit on the darknet but since wildlife trade is so difficult to regulate, it can get away with being in the open. IFAW is currently investigating hundreds of thousands of endangered species products. One big challenge is that traffickers are sneaky with their descriptions. Traffickers often use terms like “bone” or “faux ivory” when what is
being sold is actually ivory. In IFAW’s most recent investigation they found 12,000 species for sale in 5,000 advertisements. 80% of ads were for live animals, which is an increase from past years. It is still hard to figure out if these are legal, so these numbers are conservative, assuming that advertisers have documents when they say they do. Stopping illegal online animal trafficking will take strong political will and partnerships with major tech companies.

Panelists stressed the importance of innovation and partnerships in investigating cybercrime. IFAW, for example, partners with companies like Facebook and Instagram. Engaging with the private sector is key, as is using an industry-wide approach because everyone needs to be involved. Private sector companies are committed and don’t want to be linked to online crime. IFAW has highly trained spotters who observe platforms, look for suspicious posts, and flag the companies to remove them. Companies can use the information from the spotters for other types of trafficking as well, which is a bonus for them.

On the question of jurisdictional issues of global online crime, Ratliff said that the reason Le Roux could operate for so long is that the operation was inherently international even though he was selling in the U.S. Additionally, the officers on his trail were under-resourced with old computers, while Le Roux actually created his own encrypted email server. The speed with which he was operating was so out of sync with the speed at which investigators could keep up, despite the fact that the U.S. is one of the only countries that can dedicate enough resources to capture someone like Le Roux. This does raise questions though, such as what the worth of capturing someone like this is and how many resources should be put into doing so.

"The speed with which he was operating was so out of sync with the speed at which investigators could keep up, despite the fact that the U.S. is one of the only countries that can dedicate enough resources to capture someone like Le Roux."
"...what he hadn’t appreciated was the usefulness of interpersonal skills needed to deal with interagency processes and dealing with everyone’s issues and interests, which is very similar to negotiating as a lawyer in the private sector."
already a big difference between the 2018 and 2016 elections. For 2018, the U.S. government was able to take a number of steps to blunt and thwart Russia’s efforts. Asked if deep fakes are coming, Gerstell said yes and explained that deep fakes are generated videos or audios that are completely false. He said to imagine that something is posted on social media and due to artificial intelligence technology, it is almost impossible to discern deep fakes from true videos. When a candidate says a deep fake is not real, is anyone really going to believe him or her?

When asked about quantum computing, Gerstell explained that it is different from the digital computing that we now have, and that quantum computing is based on a system of sub-molecular movement that enables a vast number of computations to be done much more quickly than digital computing. In theory, if we had a quantum computer it would enable great improvements in weather forecasting and in the security area. Judge Baker added that quantum computing could be as much as a million times faster than current computers, and that artificial intelligence and 5G will also change technology. Gerstell replied that quantum computing has the potential for both good and evil, and that China has announced that its goal is to become the top country for quantum computing in the world.

Judge Baker had hinted earlier at asking him what keeps him up at night, in Gerstell’s personal view, (not NSA official policy), he is most worried about the fact that we are facing a completely unprecedented level of change in technology. AI, 5G, and quantum computing are part of an onrush of technology that is about to wash over us. He doesn’t think that our society has come to grips with the effects of this technology on our laws and on privacy, and global norms haven’t been established yet in this area. With every other means of technology that has come along—electricity, railroads, etc.—we had a couple of decades to figure out how to govern it. He said that we will have twenty billion devices connected to the internet by next year, and there are questions about what the privacy implications of that will be, what should the rules be, and if there should be a base level cyber security built into this. But unlike former technological changes, we will have to adapt laws rules, regulations, and societal norms that deal with this new technology in ten years or less.

On the question of whether the Director of the NSA should be dual-hatted (also the head of CyberCommand) as is the current Director, General Nakasone, Gerstell answered that the latter looks more
at offensive operations, while the NSA is more about finding out about our adversaries and providing information to national security systems. Each mission informs the other. In his personal view, it is likely the government will split the two roles, but not for a while.

When asked about deterrents in U.S. responses to cybercrime, Gerstell answered that there is no magic bullet or one size that fits all. The point of indicting someone overseas is that it makes it difficult for him or her to travel, or engage in economic matters, and that one such indicted person recently made the mistake of going to a country with an extradition treaty. The U.S. has taken steps to counter cybercrime, but it’s not always the case that cybercrime has been responded to with cyber means. Sanctions can also be used. The response to cybercrimes is thought of carefully at the highest levels of government and is taken very seriously. Deciding how to respond to cybercrime is a very complex, dynamic challenge.

In terms of ideas for collaborating with judicial actors, civil society, etc. as well as any ideas for the donor community in designing projects to combat cybercrime, Gerstell said that it is critically important as we face this onrush of technology that the private sector gets way more engaged than it has up until now. The private sector says the government should be helping it when, for example, China steals information or identities. The U.S. government cannot respond to this the same way that it does to traditional military threats. The private sector is the one with the information and resources at its disposal. There need to be new arrangements between the government and the private sector. A massive amount also needs to be done in education on civics, cybersecurity, and a whole panoply of things. In fact, the NSA does work with tech and media companies in the aftermath of the Russian election attacks. Some of the news media descriptions portraying Silicon Valley on the one hand and the government on the other are overstated, and broadly speaking the NSA enjoys a good relationship with the tech community.

Legislative initiatives that respond to cyber threats should be a priority, but Gerstell does not see it happening soon. He said that at some point in the distant future he could envision a treaty on international cyber norms, but we’re not there yet. There are nascent efforts by other countries to address the risks of China in the 5G area. Domestically, there are a whole series of bills in related areas. Gerstell stated that his personal view is that this is such a complicated area and that it’s coming at us so quickly that we don’t have time to try different things, analyze options, and come to a legislative solution. Gerstell said he would focus on something that would get the private sector more involved in cyber security and for the government to get more involved in the private sector, and that we need less of a divide than we have now.

"...we will have to adapt laws, rules, regulations, and societal norms that deal with this new technology in ten years or less."
CONFERENCE THEMES AND RECOMMENDATIONS

• Cyberthreats originate from three types of sources: individuals, organized criminal and terror networks and state adversaries.

• We are in a new era of great power competition in cyberspace and foreign adversaries are weaponizing digital information to undermine democratic values.

• Responses to these attacks include requiring transparency, registration, and disclosure of relationships to foreign governments to ensure that the public knows the source of information.

• Cyber attackers carefully operate below the use of force threshold to avoid reprisals from target nations.

• U.S. Law enforcement plays a crucial role in disrupting cyberattacks aimed at domestic targets and is now publicly charging nation state actors for cybercrimes.

• Attribution is an important key to deterrence.

• Public Private cooperation is essential for cybersecurity.

• Common strategies and standards for locating, accessing and preserving online data and electronic evidence are necessary for effective regulation and enforcement as everything can be deleted at the touch of a button.

• Attention to capacity building of legal actors and institutions at national and local levels is crucial to address cyberthreats.

• Election security requires thinking critically about how to protect users at all stages of the cycle (registration, campaigning, polling, election day, tabulation and certification) to ensure integrity and confidence in the process.

• We need to develop new global cyber norms about interference in other country’s processes, standards for attribution, and cooperation for enforcement mechanisms.

• Online hate speech is often coded, using culturally or politically specific slang that cannot be readily detected as dangerous by outside observers.
• Monitors should be natives of the areas they review to ensure that they can identify nuances of content

• Private, public and civil society sectors must work together to improve oversight and management of the media, including social media, and of data collection on incitement, to better protect the rights of targeted groups

• Companies should be more transparent about how they decide to remove or tolerate content on their platforms.

• Clear, elaborated reasoning would provide clarity to users and help establish precedents

• The bar is now very low in terms of opportunities to commit cybercrimes as sophisticated techniques and services have proliferated and can be purchased without any understanding of how they work

• Companies need to prepare for inevitable cyberattacks by retaining specialized counsel and being ready to conduct rapid investigations and work closely with law enforcement

• Cryptocurrency presents a problem for law enforcement because it allows individuals to transfer funds globally without any bank or regulatory institution being involved

• The long-term cryptocurrency threat is states creating their own currencies that will be completely outside of financial regulatory systems

• With many countries now requiring local data storage from tech companies we are seeing multiple sovereign “splinternets” rather than a single global internet

• The same spyware technology that helps rights-respecting law enforcement apprehend and defend against cybercriminals is also used by repressive governments interested in surveilling and harassing their critics

• We currently face an unprecedented level of technological change, including 5G and quantum computing, and we have not come to grips with its effects on our laws and our privacy.

• Global norms have not developed in this area and there is no time for a slow process