Global Information Assurance Certification Paper

CyberCrime Treaty
Greg Paulson
June 12, 2001

Introduction:

It took more than $8 billion in computer damage from the "ILOVEYOU" virus for Philippine Republic Act 8792 to come about. The country's electronic commerce act lays out how "hacking or cracking" crimes should be punished in the Philippines. Love Bug virus suspect Onel de Guzman will not face charges under the new law, rather ones already on the Republic's books that address theft and credit card fraud. The Filipino government's implementation of a new law raises the larger question of what laws are in place to address the Internet globally.

Since traditional geographical borders do not bound computer crime, problems arise for law enforcement agencies. Laws against certain hacking activities in one country may not hold water on the land of another. Lots of countries still haven't updated their laws to cover Internet-based crimes, leaving companies in many parts of the world without legal protections from malicious hackers and other attackers who are looking to steal their data.

Ongoing attacks show that no Internet-enabled business is safe. Attackers are more numerous, better armed and more talented than ever. The maliciousness of attacks is escalating, and the complexity of defending enterprises is increasing as companies engage in e-business.

In answer to these increasing illicit episodes, policy leaders from countries all over the globe are trying to beef up their laws to make bandits surfing the web pay. In order to prevent a repeat of the catastrophe that prompted this action, however, the future of the networked world demands a more proactive approach, whereby governments, industry and the public work together to devise enforceable laws that will effectively deter all but the most determined cyber criminals.

So in general, there needs to be more cooperation in trying to investigate and prosecute persons who would use the Internet to commit crimes.

This paper will introduce you to a report highlighting the current state of computer cyber laws in 52 countries. The paper will then examine a proposed new international treaty referred to as ‘Draft Convention on Cybercrime’.

McConnell Report

The study "Cyber Crime…and Punishment? Archaic Laws Threaten Global Information", http://www.mcconnellinternational.com/services/securitylawproject.cfm, conducted jointly by McConnell International and World Information Technology and Services Alliance, surveyed 52 countries to determine to state of cyber security laws around the world. Countries were asked to provide laws that would be used to prosecute criminal acts involving both private and public sector computers. In all, over 50 nations responded with information such as pieces of legislation, copies of updated statutes, draft legislation, or statements that no concrete course of action has been planned to respond to a cyber attack on the public or private sector.

The report indicates that cyber crimes, or harmful acts committed from or against a computer or network, differ from most terrestrial crimes in four ways:

- They are easy to learn how to commit
- They require few resources relative to the potential damage caused
- They can be committed in a jurisdiction without being physically present in it
- They are often not clearly illegal.

The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Effective law enforcement is complicated by the transnational nature of cyberspace. Cooperation mechanisms across national borders in solving and prosecuting cyber crimes are complex and slow, if existent! I wonder how many cyber criminals realize they can defy the conventional jurisdictional realms by originating attacks or residing in sovereign nations? Cyber criminals can create attacks from almost any computer in the world, passing it across multiple national boundaries or design attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

The report identifies ten different types of cyber crime and divides them into four categories:

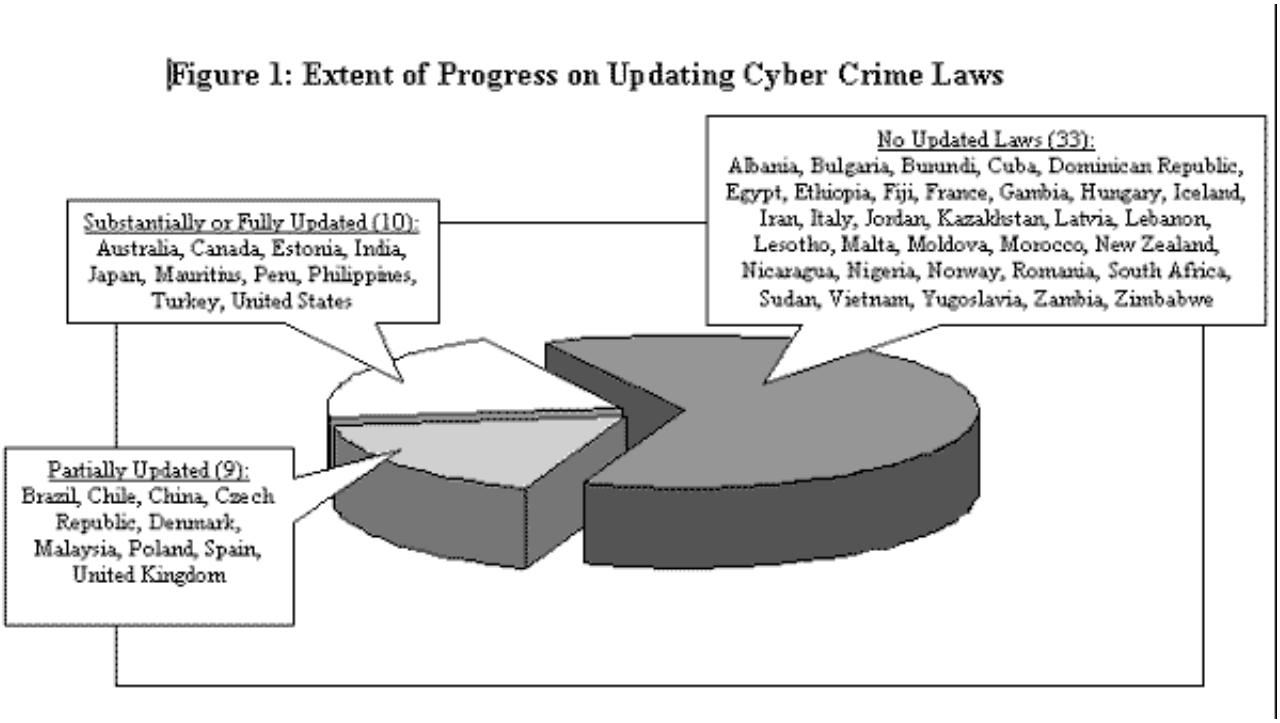
- data-related crimes, including interception, modification, and theft;
- network-related crimes, including interference and sabotage;
- crimes of access, including hacking and virus distribution;
- associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery;

Legislation, provided by each country that responded, was evaluated to determine whether criminal statutes had been extended into cyberspace to cover the above mentioned types of cyber crime.

The breakdown, according to the report, is as follows:

- Thirty-three countries have not yet updated their laws addressing any type of cyber crime.
- Nine countries have enacted legislation addressing five or fewer types of cyber crime
- Ten have substantially updated their laws to prosecute against six or more of the ten types of cyber crime.

The following figure, extracted from the study, provides a categorization of the 52 countries surveyed.



The report essentially concludes that most countries have not updated their laws on cyber crime. Companies should rely on self-protection as their first defense against cybercrimes. Only if other countries follow the examples of the leaders, those that have substantially updated their laws, will the world become a safe place for the conduct of e-government and e-business. While this seems like a nice lead in to my next topic, I do want to offer that the McConnell International report goes into far greater detail but is probably beyond the scope of this paper. I would strongly encourage adding this 'Cyber Crime…and Punishment?' report to your reading list

Draft Convention on Cybercrime

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information could create a potentially hostile environment in which to conduct e-business within a country and across national boundaries. Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-commerce. As e-business expands globally, the need for strong and consistent means to protect networked information will grow.

To be prosecuted across a border, an act must be a crime in each jurisdiction. Although local legal traditions must be respected, nations must define cyber crimes in a similar manner. Fighting cybercrime will require a well-developed network of international cooperation to effectively investigate and potentially prosecute cyber criminals. Some problems surrounding international cooperation in respective to cybercrime include:

- The lack of global consensus on what types of conduct should constitute a cybercrime
- The lack of expertise on the part of police, prosecutors and the courts
- The inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to intangibles such as computerized data
- The lack of harmonization between the different national procedural laws concerning the investigation of cybercrimes
- The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation

An important effort to craft a model approach is underway. Some countries of the global Internet community have united their anti-cybercrime efforts through a proposed treaty known as the "Draft Convention on Cybercrime". To date, the 41 member nations of the Council of Europe with the help of the US, Canada, Australia, Japan are involved in the drafting process.

The Council of Europe's ("CoE") Draft Convention on Cybercrime (Version No. 27 Revised) aims to foster a common international criminal policy that addresses offenses directed against computer systems, data or networks. The treaty is intended to encourage legislation around the world. This document is meant as an international treaty governing "cybercrime" and an attempt to standardize law for easier prosecution of attackers.

The Council of Europe in Strasbourg, France (www.coe.int) consists of 41 member states, including all of the members of the European Union. It was established in 1949 primarily as a forum to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe. Over the years, the CoE has been the negotiating forum for a number of conventions on criminal matters in which the United States has participated. Secretary General Walter Schwimmer heads the Counsel or Europe.

Brief history of the Convention on Cybercrime includes a 1989 publishing of a study and recommendations for new substantive laws criminalizing certain conduct committed through computer networks. A second study published in 1995, contained principles concerning the adequacy of criminal procedural laws. In 1997 the CoE established a Committee of Experts on Crime in Cyberspace (PC-CY) to begin drafting a binding convention to facilitate international cooperation in the investigation and prosecution of computer crimes.

The treaty has three primary sets of provisions. All three are aimed at setting basic computer-related criminal law standards for signatory nations. Signers would then bring their national laws into conformance with the treaty. This treaty could serve as a model law on cybercrime for the world!

First, it would require nations to outlaw such things as unauthorized computer intrusion; the release of viruses; and the use of a computer to commit acts that are already crimes, such as fraud and the distribution of child pornography. There is also a move to bring copyright under criminal law.

Second, the treaty requires nations to develop standard procedures to capture and retrieve online and other forms of information. Nations would have to be able to issue "retention orders" that would "freeze" data on any computer. Governments would also need the ability to capture in real time the time and origin of all traffic on a network, including telephone networks.

Third, national governments would have to cooperate with other nations in sharing electronic evidence across borders. And this cooperation requirement would apply to all crimes - not just the cybercrimes lay out in the first section of the treaty, but crimes in every signatory country

A paragraph contained in the draft's preamble was of particular interest to me, especially as a relatively new security professional. This paragraph speaks volumes to security professionals!

'*Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation;*'

The draft itself contains a total of 48 Articles broken down into chapters, sections and titles. The draft first establishes definitions for terms such as "computer system", "computer data", "service provider" and "traffic data". The draft then details, through specific articles, offenses under substantive criminal law, procedural law, jurisdiction, and international

co-operation. The draft also contains something called the Explanatory Memorandum. The purpose of this document is to help readers of the draft convention in understanding the scope and meaning of the draft's provisions, as intended by the drafters. I personally found this memorandum a huge help in sifting through all the legalese!

The timeliness of this writing coincides with the draft's potential adoption. Again, the draft was prepared by Committee of Experts on Crime in Cyber-Space (PC-CY) and will be submitted to the European Committee on Crime Problems (CDPC) at its 50th plenary session (June 18-22, 2001). The draft will then be submitted to the Committee of Ministers for adoption.

The United States accepted an invitation from CoE to participate in the convention negotiations. Due to the importance of the Information Technology sector and their vulnerability to cybercrime, the benefits to be gained from a well-crafted treaty with international cooperation, the United States assisted in treaty draft. The Department of Justice and the Department of State represent the United States. Other U.S. government agencies are also in close consultation and have actively participated in the negotiations. Cybercrime is an international problem that requires an international solution. A treaty that removes or even minimizes the procedural and jurisdictional problems that can otherwise delay international investigations and prosecutions of computer related crimes could prove extremely beneficial to the United States.

Opposition:

As with any form of legislation, the proposed Draft Convention on Cybercrime does not escape. The treaty has been strongly criticized by civil liberties group, privacy experts and industry representatives since its release. Through the Global Internet Liberty Campaign, http://www.gilc.org, two letters were submitted to the Council of Europe outlining concerns. The first letter dated October 18, 2000 http://www.gilc.org/privacy/coe-letter-1000.html and the second dated December 12, 2000 http://www.gilc.org/privacy/coe-letter-1200.html. Although the above letters addressed previous versions of the draft, they contend that little has changed with the latest draft revision. PI (Privacy International), ACLU (American Civil Liberties Union) and EPIC (Electronic Privacy Information Center) submitted the following letter http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm to the U.S. Department of Justice and the Council of Europe also expressing concerns about the treaty.

Another interesting document statement of concerns has been signed with a distinguished list of signatories including leading security practitioners, educators, vendors, and users of information security. They state bluntly, "We are concerned that some portions of the proposed treaty may inadvertently result in criminalizing techniques and software commonly used to make computer systems resistant to attack." This statement suggests that it is nearly impossible to distinguish software used in a computer crime from that used for legitimate purposes. As such, a concern with this group is that the draft treaty may be misinterpreted in the use, distribution and possession of software that could be used to penetrate the security of computer systems. The list of signatories does agree that breaking into or damaging computer systems is wrong and they do support laws against such behavior. This statement specifically targets Article 6 – Misuse of devices. Since this writing I believe provisions were included in the draft treaty to now recognize the concerns stated in the above-mentioned document. The treaty criminalizes actions that are taken "without right" or that is without authority, permission or consent. Article 6, paragraph 2 suggests that authorized testing or protection of a computer system shall not be interpreted with criminal liability as this is most likely being done 'with right' or consent. This practice lends itself nicely to the creation of a personal policy, signed by management, for the authorized use of discretionary tools for the purposes of protecting computer systems and infrastructure. One discussion thread on this subject even went so far as to suggest that security practitioners be licensed. Interesting concept!

People working with computer security are particularly affected, since much, if not all, of the software used for computer security purposes can be adapted for illegal purposes. It may even, depending on the individual's point of view, have been designed for computer intrusion, yet be an essential tool for security experts and systems administrators

During a March 6, 2001 Hearing on Cyber Crime, Bruce McConnell, President, McConnell International LLC, highlighted three concerns with the draft treaty according the U.S. private sector.

First, there is concern that the requirements placed on the Internet and telecommunications companies to assist law enforcement are overly burdensome and costly. A key area of concern is data retention. Internet service providers (ISP) are worried that they may face new obligations to hold onto data in response to requests from law enforcers. Data retention requirements could impose economic and technical burdens on many ISPs. ISPs are also worried about liability issues with respect to language prohibiting the distribution or transmission of illegal material such as

child pornography or tools that could be used to deface or disable networks.

Second, there is concern that the powers of surveillance envisioned for law enforcement officials are not balanced by comparable protections for the privacy of individuals and the rights of due process. This imbalance is viewed against a backdrop of increasing concern that the Internet is already a threat to privacy.

Third, the draft treaty is viewed as venturing into areas where existing national and international law have already been adequately established. Examples include the treatment of forgery, copyright infringement, and other offenses that are already the subject of legal protections online and offline.

Supporters:

Justice Department officials have declined to discuss their specific stance on the treaty, but in a set of FAQs posted on the DOJ's Web site http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm. The agency said while it supports the crux of the treaty, it reserves the right to interpret it with regard to existing U.S. law. The central provisions of the draft Convention are consistent with the existing framework of U.S. law and procedure. The terms of the draft Convention do permit some flexibility if other provisions do not conform completely to our current law.

The United States will make a determination whether to sign the Convention only after the drafting work has been completed and it is ready for signature. The Administration will then assess whether it is in the interests of the United States to become a party to the Convention and whether any implementing legislation would be required.

Collaborative efforts are under way in many developed countries. Representatives of the G8 group of nations, representing the world's leading industrialized countries and Russia, met in Paris and agreed to boost cooperation to fight cybercrime. Participants there confirmed their support of the Strasbourg, France-based Council of Europe's efforts to finalize a Convention on Cybercrime, which will be the first international treaty to deal with the different forms of criminal activity in cyberspace.

Lastly, Attorney General John Ashcroft also mentioned that the Department of Justice worked with our partners in foreign law enforcement to address the internationalization of cybercrime. These partnerships consisting of Group of Eight (G8) and the Council of Europe have provided us a means for discussing and developing better ways to investigate cybercrime, which cross national borders. Attorney General John Ashcroft made these remarks before the First Annual Computer Privacy, Policy & Security Institute. The remainder of the Attorney Generals comments is located at http://www.cybercrime.gov/AGCPPSI.htm.

Conclusion:

The McConnell International report showed us that most countries have not updated their laws on cybercrime. The 'ILOVEYOU' virus serves as a perfect example for the need for international legislation on cybercrime. The reality of technology is that geographical boundaries in cyberspace do not always exist. Local, state or even national boundaries do not prevent computer crime. The protection of information systems ultimately will require combinations of technical, managerial and legal approaches. No one approach will be completely effective. In order to be effective, any legislation or regulation should be sufficiently flexible to accommodate the evolving nature of computing technology and computer crime. Strict laws must be enforced to prevent those who use technology to intentionally commit crimes, attack computers and data, and those who violate intellectual property laws in that process. Security must be balanced with economics, technology and the pace of development. An effective law would be sensitive to the nature of computer crime and should not be written in such a way as to discourage research on or discussion of the technology of malicious codes. Legal issues are always highly debatable and with the proper implementation, the Draft Convention on Cybercrime could be the first international treaty covering computer-related offenses directed against computer systems, data or networks.

References:

Armstrong, Illena "Legislators Turn up the Heat on Cybercrime" SC Info Security Magazine. Volume 12 No 4 April 2001: 33-34
http://www.scmagazine.com/scmagazine/2001_04/feature.html

Thibodeau, Patrick. "Proposed cybercrime laws stir debate at conference" December 08, 2000
http://www.computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO54942-,00.html

Evans, James. "Cyber-crime laws emerge, but slowly" July 5, 2000
http://www.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg/

Krebs, Brian. "Nations Urged Not To Sign Cybercrime Treaty" December 12, 2000
http://www.infowar.com/class_1/00/class1_121300b_j.shtml

Statement of Concerns
http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_LETTER_SIGS.html

Mariano, Gwendolyn. "Global hacker agreement could affect bug hunters" October 27, 2000
http://news.cnet.com/news/0-1005-202-3314003.html?tag=prntfr

McConnell International "Cyber Crime … and Punishment?

Archaic Laws Threaten Global Information" December 2000
http://www.mcconnellinternational.com/services/cybercrime.htm

"Statement of Bruce W. McConnell – Hearing on Cyber Crime Committee on Legal Affairs and Human Rights Parliamentary Assembly on the Council of Europe" March 6, 2001
http://www.mcconnellinternational.com/pressroom/20010306.pdf

Committee of Experts on Crime in Cyber-Space (PC-CY) "Draft Convention on Cyber-Crime (Version No. 27 Revised)" May 25, 2001
http://conventions.coe.int/treaty/EN/projets/cybercrime27.htm

Department of Justice "Frequently Asked Questions and Answers About the Counsel of Europe Convention on Cybercrime (Draft 24REV2)" December 1, 2000
http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm

Yam, Jovi Tanada "Cybercrime Treaty Underway" May 3, 2001
http://enterprisesecurity.symantec.com/content.cfm?articleid=729&PID=2777476

McConnell, Bruce "International cybercrime treaty advances slowly" March 19, 2001
http://www.fcw.com/fcw/articles/2001/0319/mgt-bruce-03-19-01.asp

"Comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the Proposed CoE Convention on Cybercrime" June 7, 2001
http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm

Department of Justice "Remarks of Attorney General John Ashcroft **FIRST ANNUAL COMPUTER PRIVACY, POLICY & SECURITY INSTITUTE**" May 22, 2001
http://www.cybercrime.gov/AGCPPSI.htm

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event