Cyber security trends and predictions

New threats to security, democracy, economic growth & social stability

CANTO

34th Annual Conference, Panama

24th July 2018

Professor Anthony Clayton, CD
Chairman, Broadcasting Commission of Jamaica

BROADCASTING COMMISSION

The digital world offers many new opportunities!

Unfortunately, bad guys see it the same way…

➢ Terrorism

➢ Organized crime

➢ Fake news

- Political manipulation
- Malice, hate speech

Terrorism and social media

- IS developed strong digital media & content creation skills, use to recruit disaffected youth, raise funds.
- ..and disseminate information. EU reported 54,000 websites with information on IEDs posted online by IS August 2016 to May 2017; 2/3rd of information shared in two hours of posting.
- Hamas developed dating and World Cup apps that IDF soldiers downloaded, gave access to pictures, phone numbers, email addresses, could control the phone cameras and microphones remotely, collected sensitive information about the military.

Organized crime

Center for Strategic and International Studies ‘The Economic Impact of Cybercrime—No Slowing Down’

Global cost of cybercrime now $600 billion/year (0.8% of global GDP).
Up from $445 billion in 2014.
Rapid growth due to falling cost of entry; better use of e.g. botnets and AI; dissemination of skills, outsourcing (criminals don't need to be technologically advanced anymore, can outsource).
Costs to private firms include:

- Loss of proprietorial technological information.
- Cost of data recovery.
- Added security measures.
- Possible fines, penalties and litigation.
- Loss of confidence in company’s ability to maintain data security.
- Compromising of customer data.
- Subsequent identity theft.
- Losses to customers.
- Damage to reputation, brand.

Platform criminality

Technology platforms and social media used for trafficking narcotics, counterfeit goods, money laundering, tax evasion.

Platform criminality now generates US$1.5 trillion/year for organized crime.

Equivalent to GDP of Russia, Canada.

The Independent 20th April 2018

Q: Who ships the most weapons and narcotics?

A: The Sinaloa Cartel? ●

B: Los Zetas Cartel? ●

C: The 'Ndrangheta mafia? ●

D: The Yakuza? ●

E: The Triads? ●

F: Islamic State? ●

G: Legitimate shipping companies. ☑

Containerization: preferred by traffickers

Shipping containers are now integral to large scale narco-trafficking. About 90% of goods travel in containers, with >420 million containers shipped annually. Only 2% are inspected by Customs.

Containerization provides traffickers with the same cost- and time-saving transport mechanisms as legitimate companies.

A 2012 report by the Stockholm International Peace Research Institute found the ships involved in trafficking of weapons and narcotics are mainly commercial shipping lines. The ship owners or the captains don’t usually know what they are carrying. But it is easy for traffickers to hide weapons and narcotics in legitimate cargos.

The author said the problem is “one of the greatest security challenges of the 21st century, and so far no solution is anywhere in sight.”

2013: hackers facilitate drug-smuggling

A gang took control of computers at a harbor company and two container terminals in Belgium and the Netherlands. One of them was Antwerp, which moves over 20,000 containers per day.

They tricked staff into installing electrical power strips, external hard drives, and USB keyboards that contained key-logger software. They stole login credentials, and took control of the logistics systems.

The traffickers would hide drugs inside containers of goods from South America. The European gang could determine the location of those containers and the security codes needed to collect them, then send their crews to steal those containers before the owner arrived.

The Antwerp scheme was thought to have been running for two years before it was finally shut down, with a tonne each of cocaine and heroin seized, along with weapons and €1.3 million in cash.

It is likely that similar techniques have been used at other ports around the world.

Fake news

Political manipulation

- U.S. special counsel Robert Mueller filed indictments against 13 Russian nationals, February 2018. Members of a team that made 150,000 fake social media postings/day on YouTube, Facebook, Instagram and Twitter, using virtual private networks so postings appeared to be from USA not Russia.
- >30 countries have now reported attempts to manipulate political outcomes via social media. Some (USA, France, Germany) verified, some (UK) likely, others unknown.
- Estimates of social media impact: marginal to 1-2% of vote.

What is new about fake news?

- Lies are not new. Propaganda is not new.

<u>What is new:</u>

- Ability to mine exceptionally detailed data about every aspect of your life.
- Ability to access your contacts and their contacts to map all your connections.
- Use of algorithms to generate accurate profiles of preferences & prejudices.
- Ability to generate fake news with tailored psychological triggers designed to cause outrage [more likely to be re-posted].
- Use of botnets to generate millions of posts to blanket entire populations.
- Ability to manipulate political and social events, influence election outcomes.

➢ Traditional ‘trusted’ media losing market share to unregulated social media (social media is news source for 62% of US adults, primary news source for 18%.)

Malice

Riots and murders linked to hate speech and malicious rumors on Facebook, WhatsApp in Indonesia, India, Mexico, Sri Lanka, South Africa and others.

Example: India: social media rumors that gangs were kidnapping local children: outsiders beaten, lynched.

Example: Sri Lanka: Sinhalese-language extremists on Facebook raised mobs that attacked Muslims, destroying businesses and burning people alive.

“You report to Facebook, they do nothing,” one of the Sri Lankan researchers said. “There’s incitements to violence against entire communities and Facebook says it doesn’t violate community standards.”

Facebook has no office in Sri Lanka, which officials say makes it difficult to impose regulations.

BCJ: the direction of travel

- Support Jamaica’s transition to digital society. Ensure good media services available to all, with seamless access to diverse content across platforms.
- Facilitate positive change, mitigate harms.
- Detect and act against abuses – crime, terrorist recruitment, fake news, false advertising and electoral manipulation, grooming, bullying etc.
- Need to protect data security, prevent legitimate privacy being compromised.
- Ensure people can have confidence in information sources.
- A media and technology-literate society.
- **Need modern policy, legal, regulatory framework.** Regulatory approach: lean, transparent, efficient and effective. Content-focused, technology-agnostic. Need mix of educational and advisory interventions, legal and economic tools, sanctions and positive incentives.

Thank you !

BROADCASTING COMMISSION

www.broadcom.org
info@broadcom.org