TECHNOLOGY AGAINST CRIME, AFRICA

www.tacafrica.org

THE UNDERGROUND ECONOMY

LAW ENFORCEMENT GUIDE

· GLOBAL PERSPECTIVES FROM EXPERTS ·

Fostering innovation for future security challenges

PREVENT · DETECT · INVESTIGATE

Dr. Jerry I. Akubo

Chief Executive Officer,
Technology Against Crime, Africa

Dr. Jerry Akubo founded TAC Africa as a futurist oriented, Law Enforcement Centric NGO, borne out of an International Forum on Technologies – a high level meeting dedicated to Technologies for a Safer World, co-organized by INTERPOL and the Ministry of Interior in Lyon, France in 2013. The NGO was officially registered in Abuja, Nigeria in 2016. Prior to this, he worked over a decade and half as the National Technical Officer for INTERPOL NCB Abuja under the auspices of the Nigeria Police Force.

Dr. Akubo has been recognized by the INTERPOL Global Complex for Innovation and the Directorate of Innovation Center, Singapore for his exemplary service, partnership and contributions having actively attended and participated in over eight (8) INTERPOL General Assemblies and Eight (8) INTERPOL World Congress in a roll amongst other high level technical meetings and presentation he organized on extending INTERPOL Secured Communications Network to authorized Law Enforcement Agencies across the African Region.

He is a frequent speaker on Emerging Technologies and the maximal utilization of INTERPOL tools by Law Enforcement Agencies within the African Region while pushing a number of research and developmental projects to improve the technical know-how and easy accessibility of tools and technologies for Law Enforcement Agents especially the front line officers.

Dr. Akubo is an evangelist on the use of Innovative Aerial Surveillance, remote sensing and emerging technology to tackle most unique set of challenges the African region is facing including on the one side. Transnational Organized Cyber Crime and on the other, battling insurgents and terrorist group often domiciled in very remote & inaccessible locations.

THE UNDERGROUND ECONOMY

Changes in technology, society, and the law make new crimes possible. Attitudes are changing too. The implications of these shifts are complex. This is seen in the way law enforcement and businesses have had to adapt to deal with risks and opportunities presented by an ever-changing digital environment.

The Internet and social media have been used by criminals to carry out recruitment, solicit illegal business, and perpetrate fraud, among others. The Dark net is a part of the Internet where individuals can interact anonymously online. The Internet and the Dark net within it have enabled unprecedented globalization of crime, allowing criminals to carry out illegal business anonymously around the world, often Undetected by the authorities. Dark net marketplaces are increasingly used to profit from the processing of crime and procuring illicit drugs, weapons, and counterfeit identity documents, benefiting the perpetrators of terrorism, illicit markets, organized crime, and a myriad of other transnational crimes.

As such, many security and law enforcement leaders have stated that the emergence of the Darknet as a trading platform will see investigations focus on the clandestine corner of the internet, where criminals hide behind encryption and anonymization technology. New policing tools are needed to leverage social media to prevent and detect crimes. The future of law enforcement must adapt to a changing policing environment and societal scrutiny.

How can law enforcement better understand the impact of the underground economy? Online? How can we build better capabilities to understand and solve crimes that exploit social fault lines? What are the underlying social and technological causes of cybercrime that law enforcement needs to understand, to mitigate its effect effectively? How do criminals exploit the Darknet to enhance their criminality, and coordinate, recruit and spread their ideology? What risks and opportunities lie in? Emerging technology in cyberspace?

Managing cyber threats require addressing critical issues that law enforcement face in trying to make cyberspace safer for its users. The issues include policies, policing skills/techniques, public education, and also legislation.

CALL FOR A MULTI-STAKEHOLDER APPROACH TO POLICING

Law enforcement officials today are facing a challenging and demanding operating environment. As society is increasingly connected and the world becoming borderless, technologies can help law enforcement to prevent, detect and investigate more efficiently, but at the same time, they also open up possibilities for criminals. TAC believes that it's vision of a safer continent is possible through a multi-stake holder approach to innovation in policing.

Autonomous cars, Artificial Intelligence, robotics, drones and cryptocurrencies in the dark web; these are becoming part of today's reality, which intensifies the challenges of securing our cities, major events, borders and cyberspace.

Welcome to TAC, where we leverage new technologies to shape the future of policing. Learn, share and experience the technological possibilities and state-of-the-art policing solution in action.

Table of Contents

Nick Savvides

Information Security Specialist & Strategist
Symantec Corporation

Nick Savvides is responsible for Symantec's Cyber Security Strategy across the Asia Pacific and Japan. In this role, Savvides' charter is to provide local market insights that influence global strategic planning and product development.

Savvides works also with organizations and governments to develop their cybersecurity strategies and solve complex business problems. He has worked on some of the largest business information security projects in Australia, affecting the way many Australian's interact with their employers, banks, and governments.

An information security expert, with approximately 20 years of experience, Savvides has spent the last 10 years at Symantec in various product and sales engineering roles. He has presented at more than 60 conferences, contributed to many high profile panel discussions, and regularly appears in the media on cybersecurity-related topics.

Savvides is an active member of the IT Security community and a member of a number of industry bodies. He is a Science graduate of The University of Melbourne.

OUTSMARTING INTELLIGENT CYBER SECURITY THREATS WITH MACHINE LEARNING

Authored by
Nick Savvides

Within the lifetime of many of us, the idea that machines could learn things that humans didn't specifically teach them was the stuff of science fiction. One skim through Netflix will uncover movies of evil computers plotting to take over the world. Isn't it interesting that now that we have actual artificial intelligence and machine learning as part of daily life, one of its key purposes is protecting people and property? At Symantec, the largest cybersecurity company in the world, we see over 10 trillion security events per year and more than one million pieces of malware a day; this is an unrivaled amount of data and the ability to understand it, process it, and turn it into actionable intelligence is impossible to do using humans and traditional systems alone. This led us to develop and experiment with new technologies to tackle the scale problem, with Machine Learning and Artificial Intelligence being a key focus. This paper will discuss how these technologies have evolved and how they are applied in a cybersecurity context.

Machine Learning and Artificial Intelligence are closely related, although there are distinct differences. Machine Learning allows systems to learn from their inputs and experience without being specifically programmed, while Artificial Intelligence requires a machine to perceive and imitate human behavior. Consider a self-driving car: the system that identifies pedestrians is Machine Learning, while the whole car driving to and from a destination a dealing with all aspects is Artificial Intelligence.

Although we may be a long way from Star Trek's conversational computer, there is no doubt that machines are learning and systems are getting smarter. In the self driving car example, despite many high profile errors, more than 10 million cars with some self-driving features will be on the road by 2020. Singapore has recently kicked off the world's first driverless taxi trial in Singapore, pioneering a technology that is set to revolutionize the way we travel. These IoT-connected and automated vehicle systems can free up traveling time for commuters, allowing them to relax or work on the go, amongst other benefits.

While today's applications in digital assistants, a la Siri and friends, data mining, machine vision and industrial applications might seem amazing, but the reality is that we are in the infancy of Machine Learning and Artificial Intelligence. In reality, while these concepts have existed for 60+ years, it is only in In the last 10 years that sci-fi like advances have been made.

In terms of cybersecurity Machine Learning and Artificial Intelligence offer us a new opportunity to act as a force multiplier. The sheer scale of the threats. Devices and networks that are operated today make it impossible for humans and traditional systems to scale to understand, correlate and connect. As discussed earlier, Symantec collects more information that any single system or human could understand and this problem is only expected to get worse, as huge new networks of devices and systems roll out, each acting as both a source of an attack, a target of attack and generator of information and logs.

Consider the volume of new connected devices in the IoT that will come online in the next few years. All of these are potential vectors of attack; in fact Garter forecasts that by 2020, more than 25 percent of identified attacks in enterprises will involve IoT.

This is where we must turn to Machine Learning and Artificial Intelligence. We need these systems act as our force multiplier, as the systems that ingest all that data

and then tell only about the things we should care about and act on, making our security analysts more productive.

To date, the cybersecurity application of these technologies has been limited to Machine Learning focusing on three things: threat detection, anomaly detection, and user behavior analysis. Artificial Intelligence has yet to make a big impact on cybersecurity but this is likely to change over the next few years, as the technology matures. Let's take threat detection as an example: in this scenario, we entrust the Machine Learning system to be able to examine a new unknown file and determine if this file poses a threat.

To do this it must learn by being shown previously known bad files (convicted files), the more samples it sees, the features (attributes, components, behaviors) of those samples it sees, the more likely it will be able to detect and convict unknown files. This is a continuous process of self-improvement; new results, when validated, feed the machine and continue to improve it. The machine and the data it is trained on are completely intertwined. If we look at anomaly detection, this problem starts to become even more complicated.

It requires the system to examine patterns of behavior and automatically build profiles from what it sees. This could be in a closed system such as a self-driving car, where the system observes all of the components inside a vehicle and how they talk to each other and builds a baseline model for what is normal. When something outside of that model occurs, it's flagged as an anomaly. The ability for anomaly detection on open systems such as the internet becomes extremely difficult due to the availability of data, as it can only be truly effective if a large amount of data is sampled.

At Symantec, we take advantage of our telemetry that comes from hundreds of millions of systems to achieve this. These two things allow us to build tools that let us stay ahead of cybercriminals. Threat Detection lets us discover their new unknown malware, while Anomaly Detection allows seeing if a network or system has been compromised and if it warrants further investigation.

Our security solutions imbued with machine learning can detect anomalies mand outsmart intelligent threats, protecting us in instances where we are more susceptible but where do we go from here? As more businesses embrace digitization, the way we protect ourselves must also evolve and there is a critical need to stay proactive against threats, instead of reacting to them. With the emergence of Artificial Intelligence, we may just be able to stay one step ahead of cybercriminals.

Eventually, we will need to be able to build intelligent security systems that can not only learn faster than threats can present themselves but also be predictive of new attacks. It is foreseeable that a cybersecurity Artificial Intelligence, could observe all the outputs from Machine Learning models, looking at threats, anomalies, and even current affairs news, and detect that an attack is about to happen. This would be an amazing force multiplier for our sophisticated cybersecurity centers, making analysts even more productive.

They need to follow blogs, understand the political landscape, understand the profiles of the threat actors and even more challengingly navigate the dark web. Extracting features from files and understanding anomalies are simple tasks compared to this but an example can build Machine learning models that understand natural language. Think of digital assistants, as they become more powerful and understand what you are asking from them, the same capabilities can be adapted to a cybersecurity role, at scale.

Machines could scour the dark web and rather than looking for keywords, understand and interpret what is being discussed, in any language, and feed this into Artificial Intelligence incorporating it with all the other Machine Learning output leading to perception and ultimately detection and production.

This might sound fanciful, but 10 years ago many of the things we take for granted today was purely science fiction. While the idea of machine intelligence is ancient, its real implementation is recent. As computing power has dramatically increased while shrinking in size, increased

memory, and the quantity of data available, Al and machine learning are growing exponentially. Every time we buy something online, make a deposit or take out money from an ATM, glance at an ad, or turn on the faucet, intelligent machines are protecting us. It may not be as great a story as machines ruling the world- but it helps us all sleep better.

http://www.gartner.com/newsroom/id/3291817

Vasilios Mavroudis

University College, London

Vasilios Mavroudis is a doctoral researcher in the Information Security Group at University College London. He studies security and privacy aspects of digital ecosystems, with a focus on emerging technologies and previously unknown attack vectors. His recent publication on ultrasound tracking received wide-spread attention and is considered the seminal work on the security of that ecosystem. Vasilios is currently working towards the standardization of ultrasound communications, and designs extensions of his previous attacks. Moreover, in cooperation with industrial partners, he has recently prototyped a high-assurance hardware architecture, that maintains its security properties even in the presence of malicious hardware components.

In the past, he has developed auditing tools for the Public Key Infrastructure of Deutsche Bank and participated in an international consortium studying large-scale security threats in telecommunication networks. Furthermore, he has cooperated with UC Santa Barbara in several projects, including a detection system for evasive web-malware. Vasilios holds an Information Security MSc from UCL, and a Bc in Computer Science from the University of Macedonia, Greece.

OUTSMARTING INTELLIGENT CYBER SECURITY THREATS WITH MACHINE LEARNING

Authored by
Visilios Mavroudis

Executive Summary

In the last few years, unlawful activities on the Darknet have become a major challenge for law enforcement agencies, as criminals use them increasingly often, knowing that identification of individuals is far from trivial. To address this problem, we introduce a new set of law enforcement tools that can be used to uncover the identity of criminals in anonymity networks and services (i.e., the Darknet).

These tools are highly effective, and are based on an emerging digital ecosystem that uses inaudible audio signals to link the different devices owned by a user. Compared to existing solutions, whose success rate in real-life conditions has been proven quite limited, our techniques do not rely on vulnerabilities in the darknet software or design. Instead, they utilize the capabilities provided by the ultrasound ecosystem to create a high-accuracy link between the anonymous identity of the criminal and his real one.

Currently, Tor is the most popular anonymity network that enables users to both browse websites and hosts their services, while hiding their real identities. Due to its popularity, Tor handles the great majority of "anonymous" traffic and is estimated to host approximately 30,000 hidden services.

Not surprisingly, Tor and the darknet in general, serve as a major hub for various kinds of criminals, as it allows them to conceal their activities, and more importantly protects their identity from law enforcement. This allows criminals to maintain pseudonymous Darknet identities and use them to build a reputation in their underground community. Such behavior is most commonly observed in Darknet trading venues, where the users buy and sell illegal goods and services and try to build and maintain reputable profiles to increase their revenue. Unfortunately, even when law enforcement traces these illegal platforms, the identification of the criminals remains a challenge. In this context, our techniques realize a new way for authorities to deanonymize criminals who visit the Darknet websites and resources. To achieve that we developed a set of tools that use popular ultrasonic applications to transmit a unique identifier from the "anonymous" device used by the criminal, to nearby devices that have not been anonymized.

For instance, cross-device tracking and proximity marketing application deployments can be used to trigger specific functionality in the criminal's smartphone, by remotely injecting specially crafted inaudible tags. Moreover, it should be noted that in most cases the users are not aware that their device is listening for ultrasounds, as this functionality comes as part of a third-party framework incorporated in the app. In addition to these, we also extended our techniques to operate in an offline fashion, so that they can be used in physical, real-life encounters, where connectivity is not always assumed.

All in all, the ultrasound ecosystem already features a wealth of applications and is expected to expand further in the next two years along with the number of participating users, which we currently estimate to be at least a few million. Consequently, the coverage and the effectiveness of these techniques are expected to also increase with the number of devices listening for ultrasounds, thus providing a robust way to uncover criminals residing on the Darknet.

Nils Andersen-Roed

Operational Specialist / Project Leader
Darkweb Team
Dutch National Police

Nils Andersen-Röed is an Operational Specialist and project leader for the recently started Darkweb Team of the Central Unit of the Dutch National Police. One of the main goals of this team is to impair trust in Darknet markets and anonymity and security on the darkweb in general. Andersen-Röed joined the Dutch National Police in 2011 and, after receiving his Master of Criminal Investigation degree, has been working as an investigator and counter-thinker at the National Crime Squad. Before joining the National Police he received his Masters's degree in Psychology and was working as a network professional in the private sector.

DARK WEB INVESTIGATIONS - AN OVERVIEW FROM THE DUTCH POLICE

Authored by
Nils Andersen-Roed

The dark web is the part of the deep web the non-indexed part of the internet) where people can surf anonymously. The dark web consists of several different Darknets such as Tor (The Onion Router), Freenet, and I2P (Invisible Internet Project), Openbazaar or Zeronet Access to the dark web needs a special browser.

Tor is currently the most commonly used network, and it can be accessed by using the Tor Web Browser allows the identity and the location of the user to stay anonymous due to the use of a multi-layered encryption system. It is also possible to host services on the Tor network, known as the Hidden Services. If the server of the Hidden Services is configured correctly, both the physical location of the server and the identities of the users remain hidden.

The Hidden Services are commonly used to host Darknet markets. Vendors and buyers on these platforms can contact each other to trade (mainly illegal) goods, such as drugs, weapons, counterfeit documents or money, cybercrime tools, or stolen credentials. Communication between vendors and buyers usually takes place via PGP (Pretty Good Privacy) encrypted messages and the purchased goods are paid in crypto currency like Bitcoin, Monero, or Ethereum. In addition to the vendors, administrators of Darknet markets also earn a percentage (usually 2 to 5 percent) for each sale that is made on their market.

Currently, the most popular Darknet markets are Alphabay, Valhalla, Dream Market, Hansa Market, and Acropolis Market. In the last couple of years, Darknet markets have grown substantially and the yearly revenue of Darknet markets is estimated to be several hundreds of millions of dollars.

According to a recent study by RAND Corporation (2016)', revenues from Dutch vendors are by far the largest on a per capita basis compared to vendors operating in the The United Kingdom or the United States, and specialized in selling ecstasy (MDMA)- type drugs and stimulants.

Dutch police investigations have also revealed that in addition to selling drugs on Darknet markets, some online vendors agreed to face-to-face meetings with their buyers to sell larger quantities of drugs in the physical world. It is not known how often these kinds of meetings take place and the quantities that are being sold.

Besides buying and selling drugs, it is also possible to buy weapons and explosives on Darknet markets. Other Hidden Services consist of websites that offer assassination services, money laundering services, and child pornography, or terrorism-related information.

Due to the recent growth of illegal Darknet markets, the Dutch National Police have formed a dedicated dark web unit to combat crime on the dark web, impair trust in Darknet markets, and overcome the anonymity and security on the dark web. In recent years, the Dutch National Police have investigated over 50 dark web-related cases. About half of the cases were drug-related, and about a quarter involved the purchase of weapons or explosives. These investigations revealed that vendors located in the Netherlands are typically selling drugs, while Dutch buyers are mainly purchasing weapons and explosives. These investigations were launched either due to information received from foreign law enforcement agencies or leads on suspects identified by the investigative units through Big Data analysis or the inception of shipped parcels.

The trading of illegal goods on the darknet can be divided into four different phases: production; online vending of the illegal goods or substances; transportation; and financial transaction in which virtual currency is converted to fiat currency or goods. Police investigations can focus on all four phases to identify vendors. Several tactics and strategies can lead to the successful identification of suspects, mostly through the combined use of digital and traditional investigative methods.

For example, investigators from the Dutch National Police have successfully identified a vendor through the use of undercover tactics of acting as a buyer to make test-purchases while concurrently infiltrating the forum of the Darknet market to become a trustworthy partner to the vendor. After gaining enough trust, a face-to-face meeting was arranged where the identity of the vendor was revealed. Several other cases were solved through the analysis of text messages- between vendors and customers which were gathered during previous police operations.

Some of these messages contained useful details about the location of the vendor, meeting places, telephone numbers, PGP keys, information about their social life, or information about their appearance. In one case, the combination of the information on the location where the vendor met with his customers and a news article about the vendor's family on a local news website in the same region led to the successful identification of the vendor. The Dutch National Police are also actively working together with the parcel delivery services.

When packages with illegal substances are detected during parcel inspections, their return addresses or track and trace codes are investigated to find out which postal offices the parcels were sent from. By tapping on CCTV surveillance and employing physical surveillance in the neighborhoods of these postal offices, the identities of the vendors were successfully established.

A dedicated post parcel intervention team has been formed to focus on the investigation of such intercepted parcels. The police can also combat darknet related crime by focusing on the money trail of illegal transactions. For example, the Dutch National police have successfully identified a bitcoin-to-cash exchanger that was active on the bitcoin exchange platform localbitcoins.com.

Tactics that were used consisted of a combination of bitcoin transaction analysis and traditional investigative methods such as analyzing CCTV footage and investing traditional banking transactions. Besides focusing on identifying vendors or criminal bitcoin exchangers, the Dutch National Police are also developing new methods to identify the physical location of Darknet markets to target the markets directly. Although previous takedowns of Darknet markets have produced valuable intelligence, new markets have emerged to fill the gap and enable vendors to continue with their businesses.

Therefore, the Dutch National Police are also working on developing innovative methods to tackle this problem. In October 2016, the Dutch National Police and the Dutch National Prosecution Service have launched a Hidden Service on the Darknet. The Hidden Service (https://poli epcvh42eav. onion) features information on the detection and prosecution of many large vendors who operated on Darknet markets.

It also points out that the buyers of illegal goods on the Darknet are not as anonymous as they might think. In sum, the level of difficulty in Darknet investigations is comparable to traditional investigations if a combination of digital and traditional investigative methods is used. However, the Police's successes are contingent on the criminals making mistakes. Fortunately, the internet never forgets when criminals make mistakes.

Maria Vello

Certified Information Systems Security Professional (CISSP)
Chief Operating Officer
Cyber Defence Alliance

Ms. Maria Vello, CISSP, joined the Cyber Defence Alliance (CDA) as Chief Operating Officer in April 2016. Prior to this she was CEO and President of the NCFTA (National Cyber-Forensics & Training Alliance) for three years. Maria has been recognized by the FBI Executive team and FBI CIRFU for her exemplary service, partnership, and contributions to the Cyber Division. She has been recognized by the NCFTA for her exemplary leadership, dedication and unparalleled passion for the NCFTA mission. Awarded the AT&T Leaders Council award for being in the top 2% at AT&T, she was the also the number one Regional Security Manager at Cisco Systems, number one AT&T Sales Manager and she was also named to the top ten women in Cloud in 2014.

Maria brings a wealth of experience in trust-based collaboration, information sharing across industry, law enforcement, government and academia to proactively detect, protect, deter, dismantle and stop cybercrime or threats. She has effectively led tears to leverage cross-sector resources and threat intelligence to more effectively analyze, correlate and attribute critical real-time intelligence against emerging cyber threats and deliver actionable intelligence to both industry and law enforcement.

TACKLING CYBERCRIME - ONE CHALLENGE AT A TIME, COLLECTIVELY AND COLLABORATIVELY

Authored by
Maria Vello
Micheal Shoukry

The cyber Defense Alliance (CDA), is a non-profit public-private partnership focused on the collective and collaborative sharing of information and intelligence at an industrial level to fight cybercrimes/threats and provide actionable intelligence for our members and partners.

The CDA has been able to pave the way for an unprecedented level of information sharing to tackle cybercrime. The CDA has proven, that it is only through earned and sustained trust in a purpose-built environment that you will truly share at the levels required to be ineffective in this war on cyber threats/crime.

Through this unprecedented and real-timesharing the CDA has been able to demonstrate that by collectively and collaboratively working together we can accelerate our knowledge, innovation, capabilities, and preparedness. We also know that no one tool can enable the transformation of data into intelligence and ultimately into action. However, through the application of the collective efficacy model within a purpose-built trust environment, the CDA has been able to combat cybercrime.

The pace of cyber threats is astonishing and this is a systemic and global problem. In today's ever-changing threat landscape, the only way to tackle significant and highly distributed threats is to accelerate our pace through trust and a unified model, to pool our resources, information, and knowledge, globally.

Taking the above approach is not always the easiest as there are challenges of differing legislation, policies, and governance models across countries, organizations and borders. In addition, the laws around extradition, prosecution, and law enforcement agencies working together can be challenging and cumbersome.

The Mutual Legal Agreement Treaty (LAT) process is not always conducive or fast enough in cyber, especially when being expedient is critical.

However, through this unified, collaborative trust model, the CDA has proven that trust model can stop imminent attacks before they happen, identify malicious actors, and ultimately arm law enforcement with the necessary intelligence to dismantle criminal enterprise organizations, their infrastructures, and arrest malicious actors and seize their assets for long term impact. Cybercrime can have devastating impacts on organizations, individuals, economies, and governments.

The threat landscape is constantly increasing, the problems are constantly evolving, and the threats are increasing from the basic spam, advertising, Nigerian scams, social engineering, and phishing scams, to extremely sophisticated exploitation of vulnerabilities leading to ransomware, zero days, and much more. But why does this gap exist and continue to widen? And how can we collectively shrink this rapidly widening gap and fight cybercrime at scale?

Why does the gap exist?
- Is it a lack of education or knowledge?
- A deficiency in understanding the risks;
- A lack of sharing;
- A lack of resources, skills, and expertise;
- A lack of tools to combat such threats;
- An increased number of vulnerable systems/code;
- Amount of sophisticated exploits and exploitation tools leaked;
- Innovative threat actors;
- New emerging technologies and capabilities (IoT devices, easily accessible cloud computing systems, etc.);

• A gap in in-laws;

• The penalties/implications of getting caught are not severe enough;

• A gap in enforcement of law enforcement capabilities to combat such crimes

• Legislation and regulations have not kept pace with the times or adverse implications of the internet; The darknet;

• Offline secure encrypted communications, (obfuscation) We could go on, the list is immense; or is it simply all of the above?

When we look across the above items as to why this gap may exist, the answer becomes somewhat overwhelming, especially since many are difficult to measure through tangible means at a global level. However, the only clear answer is this solution is highly likely decentralized across both the private and public sectors and many industries and the globe.

By reflecting on past successes of both traditional law enforcement (drug cartels, terrorism, crimes against children, etc.) and cybercrime (botnets, silk road, criminal forums), we quickly recognize that solving this global problem requires international collaboration through private-public partnerships. Many cybercriminals are opportunists always looking to take advantage of the circumstance to exploit easy targets, the classic example of this is "an older person looking for love", or a simple phishing email, both of these have been around for over a decade and are still being employed by malicious actors. But why do these attacks continue to get used?

These attacks are only continuing to be used because they are successful. If such attacks were not successful, malicious actors would quickly pivot to the next opportunity. Of course, as new opportunities for more sophisticated attacks arise, the attackers will quickly begin adopting them, for example in more recent cases, attackers leveraged vulnerabilities in software to build wormable ransomware and impacted thousands of people (Wannacry).

Cybercriminals are always looking to enhance their business model and as innovations emerge, criminals utilize technology just as those security practitioners and general technologists in our industry do to become more profitable and scale their criminal enterprise. Enterprise groups are the poster child for why and how information sharing can be extremely effective. They have dramatical, improved their pace, innovation, knowledge, and capabilities to elevate their game and gains. They have the best sharing model on the planet- we can learn from them. They know us better than we know ourselves, they know our thresholds, limits, and systems.

They know our rules and regulations better than we do, when we come out with new rules, and regulations best practices they do an exceptional job of communicating that information to each other. One example is NIST in the us. When NIST was finally published, within days, it was made available in the underground market to all the cybercriminals, translated into multiple languages. The darknet/dark web "marketplace" has certainly played a role in increasing the pace and magnitude and escalation of cybercrime and it will for a long time.

However, it is getting increasingly difficult to leverage it to gain actionable/evidential intelligence for some of the very serious organized crime groups and get into the vetted forums. You have to pay to play with the advanced, experienced, sophisticated groups and forums. You have to demonstrate your value and actually commit the crime in a number of the groups. Even in the dark criminal marketplace, there are ratings for trust.

However, it is getting increasingly difficult to leverage it to gain actionable/evidential intelligence for some of the very serious organized crime groups and get into the vetted forums. You have to pay to play with the advanced, experienced, sophisticated groups and forums. You have to demonstrate your value and actually commit the crime in a number of the groups. Even in the dark criminal marketplace, there are ratings for trust.

The ability of criminals to take conversation off-line into private secure chats, secure communications, and obfuscate themselves is far too easy. As new tools and technologies emerge, criminals will quickly look to adopt them and leverage them to enhance their operations.

This is shown by how innovations such as TOR, P2P, blockchain, anonymization services, encryption, secure communication software, etc., are being used by cybercriminals. Criminals a have used the above technologies and others to develop their Software packaged in an “as a Service" model (Also referred to as Ransomware as a Service), offering business analytics dashboards, and a till platform for any novice threat actor no launch an attack.

With the increased accessibility of these criminal services, the attacks will continue to be on the rise. By attempting to go after each one of these tools or services, we quickly realize that this becomes a game of "Whack-A-Mole" that won't lead to the desired long-term impact. This global problem only gets more challenging as we take a look at varying laws, regulations, and a decentralized law enforcement eco-system.

Varying data and privacy laws, regulations, and a lack of consensus among lawmakers add a whole new complexity to this challenge.

While there is no dispute that privacy, laws, and regulation are a necessity, we must collectively agree to streamline the processes and develop balanced and flexible regulation to support the fight against cybercriminals who have a total disregard for the law and simply do not adhere to governing principles. We must preserve the balance in maintaining a safe, secure, and transparent cyberspace, and à complex challenge such as this requires a collective approach that is built on trust. The Internet is borderless, and cybercriminals use this to their advantage.

Cybercriminals use laws and any regulations that we place on information sharing to their advantage. We must maintain a balance to protecting the privacy of non-malicious Individuals; it's also critical that we collectively agree on policies and legislation that allows the exchange of information through public-private channels for the right reasons and intent.

Through education, situational awareness, changing our behaviors, truly sharing our resources, information sharing, public-private partnerships and securing our systems across the globe, only then will we be able to put a dent in cybercrime and cripple cybercriminals.

Raising the cost of committing crimes reduces their return on investment, increasing the severity of the penalties, increasing the probability of getting arrested and prosecuted, and lowering the likelihood of successful malicious exploitation, only then will the scale begin to tilt in our favor. Should there be norms, how do we get these done on a global basis? We have only discussed the challenges around cybercrime, what about the Nation States, the political implications, and our inability to extradite in some countries? There are many areas to address and we will over time, but time is of the essence.

It is not just financial aspects of cyber we should be troubled about and focused on, but also our intellectual property, patents, research and development, mergers and acquisitions, the ability to influence countries' elections, recruitment of people, and more importantly the ability to distinguish between the truths, what is real, and what is fact.

This fight against cybercrime is a threat to our economies, and critical infrastructure and attacks can lead to devastating impacts. We must come together, unify our forces, pool our resources, and knowledge, increase our preparedness, and make forward progress in raising the difficulty for criminals to operate in cyberspace.

Every one of us has a moral obligation and plays a critical role in helping to neutralize cybercrime/threats and focus on building a safer cyber future. There is not one company, agency, or country that can fight this war alone.

The CDA Team

Jim Pitkow

Chair Technical Task Force
Thorn

Jim is a serial entrepreneur who specializes in translating emerging technologies into practical applications. As the Chair of Thorn's Technical Task Force, he has worked with commercial partners to develop innovative solutions to fight the sexual exploitation of children including the Industry Hash Program, Project VIC and Spotlight. Jim started his career prototyping some of the first uses of the Web for NASA then as a Research Scientist at Xerex PARC. He received his Ph.D. in Computer Science from Georgia Institute of Technology.

CHILD SEXUAL ABUSE THRIVES IN THE DARKEST PARTS OF THE INTERNET

Thorn: Digital Defenders of Children

Authored by
Jim Pitkow

It is not every day that you are called upon directly to change the course of one individual's life in a clear, purposeful way. But when you are, it stays with you. And, when you fail, it sucks even harder.

Three years ago, our organization, Thorn, was called upon to help law enforcement identify a child whose images were being distributed in a child abuse forum operating on the Darknet. By the time investigators began the search, the girl's images had been circulating for more than two years.

Because the perpetrators operated on the Darknet and had removed all identifying information from the images, investigators had little information to work with. Thorn was asked to assist in finding advanced facial recognition tools that could help match this little girl's face to publicly available data on the Open Web to find her quickly.

Existing technologies could not easily scan major public image databases at scale to help identify the child. We failed and her abuse continued for another year and a half. Finally, investigators were able to use other clues to find this child.

Over the 5 years of this child's abuse, nearly 1,000 images and videos of this child were distributed in the Darknet, and are now open circulation joining the millions of other children sexual abuse images that feed the growing demand for abused content globally. This is a prime example of the darkest side of innovations and illuminates the need for investment to combat abuse and exploitation as new technologies emerge.

Over a decade ago, the United States Naval Research Laboratory created a tool- TOR for the purpose of protecting naval communication online. Tor is free software that enables anonymous online communication. It transmits communication through a global network of thousands of relays to protect a user's location and identity. The network it creates is often called the Darknet.

The benefits of this technology go beyond protecting military communications to providing a secure way for vulnerable members of society (e.g., political dissidents, citizens of oppressive governments, whistleblowers) to communicate over the Internet, and avoid possible observation or retaliation. There are many good and noble purposes for this technology.

Yet, as with so many innovations, there have been unintended consequences. Political dissidents are not the only ones using internet anonym zing tools, like Tor. Such tools are also being used by criminals and exploiters, including human traffickers, weapons traffickers, drug traffickers, child abusers, and many others.

Today, the anonymous Darknet has become an open market for the trading of the most extreme child sexual abuse content. Because the Darknet is not indexed and sites are unreliable, it is difficult to measure the the exact size of the child sexual abuse material marketplace, but a recent study by Daniel Moore and Thomas Rid, both of King's College London, have attempted to do so.

It is estimated that while child sexual abuse sites account for between two to three percent of the sites on the Darknet, they account for around 80% of Darknet traffic. We know that there are hundreds of sites (not all active at any given time) that may host child abuse content, and there are hundreds of thousands of images and videos of child abuse being published in this environment each year.

The Darknet poses a multitude of challenges for investigation and identification. TOR is not indexed and therefore not searchable. It is difficult to identify new sites that are used to discuss and distribute child sexual abuse material. New sites come up and sites go down temporarily or definitively, leaving no trace of the digital footprint of abuse.

Files shared on file sharing sites 'time out'- each shared file needs to be downloaded within a short period after it is uploaded. Knowing who' is who' and how they are associated (admins, content producers, clients, etc.) takes a significant amount of time to determine. Identification of new victims or a new image associated with a victim is next to impossible to keep up with.

At Thorn, we are working to address these challenges and to provide law enforcement with the tools needed to surface intelligence that leads to the quick identification of victims of child sexual abuse material, as well as the key actors that produce and promote this material on the Darknet. Our work focuses on detecting new sites, collecting data, prioritizing information, connecting disparate pieces of information to make sense of the bigger picture, integrating identification tools, and improving collaboration globally. The key to success in this work is leveraging advanced technologies that are already deployed in other fields.

We're able to tap into private industry investments through our Technology Task Force, such as Microsoft's work on age progression and facial recognition through Project Oxford. In addition, we turn to government investments as well and have looked to the research coming out of the DARPA MEMEX project to inform discovery and collection. The overarching goal is to co-opt the best and brightest minds in IT and harness the most advanced technologies on behalf of some of the world's most vulnerable children Today, governments around the world spend millions of dollars on innovation focused on defense and yet the teams working on behalf of these children are often left with decades old technology at their disposal.

As a none. Profit organization, we are closing that pap by building new applications via our dedicated production teams, and connecting the dots between existing public and private Investments that can make dramatic changes in this field.

In 2014, we released our first product, Spotlight, which helps law enforcement identify child sex trafficking victims sold online. Today, that product is deployed across the United States and Canada and has helped identify more than 6,000 victims of trafficking. It has also helped cut law enforcement investigation time by more than 60%. It is transforming the way these investigations are handled _ bringing the needle in the haystack to light quickly and giving investigators the information, they need at their fingertips.

The work we're doing on the Darknet has a similar focus. Our tool, Solis, is currently being tested in eight countries with federal agencies that specialize in Darknet child abuse investigations. Our goal is to never let another child linger online for years with the world watching her abuse. We will arm front line investigators with the tools they need to focus on new abuse quickly, and put at their disposal the full range of technologies to help identify and rescue victims.

Join us in this mission at www.wearethorn.org.

Benjamin Ang

Senior Fellow
Center of Excellence for National Security
(CENS)
S. Rajaratnam School of International Studies
(RSIS)

Benjamin Ang is a Senior Fellow at the Center of Excellence for National Security (CENS), S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. He leads the Cyber Programme of CENS, a team whose research areas include international cyber norms, cyber deterrence, cyber state governance, hybrid warfare and influence operations, cybercrime, smart city cybersecurity and governance, data privacy, and cyber issues in artificial intelligence. He also serves on the Executive Committee of the Singapore Chapter of the Internet Society, the international non-profit organization that is the trusted source of leadership on Internet policy, technology standards, and future development.

He draws on varied experiences as a litigation lawyer in one of Singapore's largest firms, CIO in a multinational professional services firm, legal counsel in media and technology companies, and as a technology consultant.

TACKLING TRANSNATIONAL CYBERCRIME WITH MUTUAL LEGAL ASSISTANCE

Authored by
Benjamin Ang

International challenges of cybercrime
International challenges of cybercrime A recent INTERPOL investigation ide

Many countries have passed legislation that provides jurisdiction over cybercrime activity affecting their citizens or property, even if the criminals are located outside the country's borders. However, merely criminalizing transnational cybercrime is not effective. Successfully combatting cross-border cybercrime, however, requires more than just criminalization.

Success requires effective international cooperation. Unfortunately, International cooperation in cybercrime cases comes with well-known challenges.ntified nearly 9,000 servers in Southeast Asia that are being used for cybercrime, including command and control for malware, launching distributed denial of service (DoS) attacks, spreading ransom ware, and sending spam, with victims and suspects in China, Indonesia, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

There are also documented cases of cybercriminals based in Romania, Estonia, Lithuania, and Russia, who have committed large scale crimes ranging from 'phishing' (sending millions of emails luring users to fake banking websites to steal their banking passwords), theft of credit card numbers and ATM PINs, computer intrusion, wire fraud, illegal appropriation of money, and installing malware that intercepts bank account passwords.

In all of these cases, the criminals committed their crimes without ever physically stepping into the same country as their Victims. They illustrate how global technology can be used for committing criminal acts with a transnational reach, posing a huge challenge for local law enforcement. Fortunately, there are international legal instruments that local law enforcement can use to address this challenge.

Foreign authorities may be reluctant to recognize legal traditions and systems, particularly if they are requested to assist in a manner that is different from their national law or principles. States are also naturally reluctant to transfer their citizens to another state for criminal prosecution. Some countries rely upon a tradition of non-intervention and may view investigation assistance as burdensome or intrusive absent a treaty for cooperation.

Conventions, Treaties, and Mutual Legal Assistance International law enforcement cooperation can be either formal or informal. Formal mechanisms include bilateral or multilateral treaties for mutual legal assistance. This is the process by which States request and provide support in criminal cases.

The largest global cybercrime cooperative agreement is the Council of Europe's Convention on Cybercrime ("Budapest Convention"). Article 22(1) (a) of the Budapest Convention requires signatories to recognize computer crimes that are committed in their territory, while Article 23 requires signatories to provide cooperation to the widest extent possible, including collection of evidence.

Another important instruments are the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime within ECOWAS, Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information, Shanghai Cooperation Organization (SCO) Agreement on Cooperation in the Field in International Information Security, African Union (AU) Draft Convention on the Establishment of a Legal Framework Conducive to Cyber security in Africa, and League of Arab States (LAS) Arab Convention on Combating Information Technology Offences. In addition to the Budapest Convention, individual national Mutual Legal Assistance Treaties (MLAT) treaties have established streamlined procedures for

rapid cooperation between law enforcement authorities.

Time is of the essence in combating cybercrime, as computer evidence is highly volatile and easily destroyed. These treaties provide for expedited preservation of evidence and disclosure of stored computer data. They may also provide mutual assistance in the real-time collection of traffic data, and the interception of content data. To implement these forms of assistance promptly, states also agree to designate points of contact who can be reached on a 24/7 basis.

Other contact resources include the UNODC Online Directory of Competent National Authorities, Commonwealth Network of Contact Persons, European Judicial Network, and Euro just. Limitations to Mutual Legal Assistance Mutual Legal Assistance treaties are still not a magic bullet, as many agreements and domestic legislation place limits on mutual legal assistance. Some of the situations where assistance will not be provided include acts that are political offences, acts that are not criminal offenses in the assisting state, and instances were implementing the request could violate the assisting state's sovereignty, security, or order.

Despite these limitations, law enforcement agencies in many countries have found success in transnational cooperation to combat transnational cybercrime. The most well-known examples are US law enforcement officials who have successfully cooperated with their counterparts in Lithuania, Estonia, Spain, and Bulgaria, arrested several cybercriminals and in many cases extracted them to the USA for trial. These and many other unsung heroes are good indicators of the effectiveness of cooperation and international legal instruments in the battle against transactional cybercrime.

STRONGER ENCRYPTION OR WEAKER ENCRYPTION FOR PUBLIC SAFETY?

Authored by
Benjamin Ang

In the wake of terror attacks around the world, government leaders, including those of France, the United Kingdom, USA, and Australia have condemned strong encryption- the technology that keeps data and messages hidden From third parties- as hindering efforts to combat terrorism and crime, On the other hand, technology, and security experts have criticized such calls to weaken encryption, arguing that weakening encryption would not only fail to prevent terrorism and crime but Would instead cause greater insecurity for the public.

The case for weaker encryption

From a technical perspective, any device or application that can be penetrated on demand is considered to have a 'back door' for entry. However, since the term has its baggage, this article will use the term weak encryption' instead. Surveys in the USA have indicated that the public would favor weakening encryption if that would enable law enforcement to investigate and prevent terrorists and criminals from striking. One example would be messages that the Westminster attacker Khalid Masood sent on WhatsApp just minutes before he launched his assault that killed four people. Presently these messages are encrypted and cannot be accessed even by the WhatsApp Company.

Officials argue that such terrorist attacks would be easier to prevent if authorities could penetrate encrypted services like WhatsApp, just as they used to listen in on telephone calls or steam open letters and read their contents. The safeguard would be that the police or other authorized agency would need a warrant through the proper channels.

In this light, it appears perplexing that Apple and Google announced that their iPhones and Android smartphones will be encrypted end- to-end by default i.e. all the data stored on the phone itself will be unreadable to anyone who accesses the phone without the device passcode, passcode, and even they (Apple and Google) would not have access. Why would they do such a thing?

The case for stronger encryption

Firstly, it is argued if WhatsApp, iPhones and Androids have weak encryption, this would not deter terrorists. The terrorists who attacked Paris used prepaid burner phones, not encryption, to keep off the radar of the intelligence services. After the attacks, investigators found the phones with a detailed map of the concert hall and an (unencrypted) SMS messaging saying "we're off; we're starting." Investigators found evidence that ISIS supporters are disinterested in using encryption to hide their web browsing activities, or to create a secure version of propaganda websites.

Terrorists and criminals who want to hide their communications will still have a wide range of strongly encrypted apps and tools, easily available from other developers. Signal, Telegram, Threema, and ChatSecure are only the tip of the iceberg. ISIS has made its encrypted messaging app called "Alrawi".

Secondly, it is argued that weak encryption will expose confidential data (banking data, passwords, trade secrets) as well as critical infrastructure (banks, power grids, telecom), to risk. The US House Homeland Security Committee acknowledged in their report that creating a means for law enforcement to get access to the data stored in Google or Apple phones "would naturally be exploited by the bad guys- and not just benefit the good guys."

The fundamental problem is that if one government can penetrate encryption to access a device, eventually so will malicious hackers, identity thieves, and foreign (possibly unfriendly or corrupt) governments, thereby actually enabling cybercrime and undermining national security. This happens because any encryption which can be

be penetrated therefore has a vulnerability, and cybercriminals have many nefarious ways to find vulnerabilities. One example is the ransomware attack named WannaCry affected businesses, hospitals and governments of more than 150 countries, using vulnerabilities stolen from the National Security Agency, the USA's top spy organization.

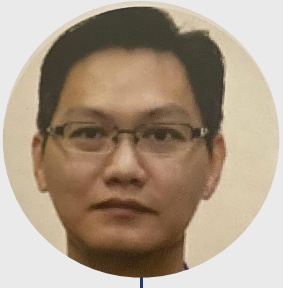
One may trust one's government to properly safeguard the ability to penetrate one's encryption, but one must also remember that every other government in the world will also have the same ability, because technology companies must grant access equally. When geopolitical conflicts arise, this would be detrimental to national security.

Thirdly, any security weakness in our increasingly complex network environments can be exploited by cybercriminals, to infiltrate critical systems like banking systems. When bank statements for Standard Chartered Bank's wealthiest clients were found on a hacker's laptop, they had been stolen not from the bank's highly secure servers, but from a less secure server at the company which prints the bank statements. Particularly in the financial sector, encrypted communications provide confidentiality as well as authentication, which is required for secure transactions. Any cybercriminal who can penetrate encrypted communications will also be able to forge them.

Public safety

Even in other sectors, researchers keep finding malicious software that can shut down electricity grids, pacemakers, and the brake systems of cars. As more devices like smart cars and smart homes become connected online, as part of the Internet of Things, it appears that stronger security everywhere, not weaker, is needed to protect public safety.There may be technologies in the future that enable encryption to be penetrated safely.

Perhaps (and this is wildly speculative) quantum cryptography, where the act of reading data encoded in a quantum state changes the state, would enable users to detect eavesdropping in quantum key distribution, even distinguishing between lawful authorities and cybercriminals or enemy states. In the meantime, with the present state of technology, public safety is better served by encouraging technology companies to make devices and applications with stronger encryption, not weaker encryption.



Tan Teck Boon

Research Fellow in the Office of the
Executive Deputy Chairman
S. Rajaratnam School of International Studies
Nanyang Technological University,
Singapore

Teck Boon is a Research Fellow in the Office of the Executive Deputy Chairman, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. His research covers smart cities governance, policy implications of emerging science and technology as well as inter-organizational cooperation and information sharing. He obtained his PhD from the Lee Kuan Yew School of Public Policy, National University of Singapore (NUS). He also holds a Master of Social Science from the Department of Economics, NUS, and a Bachelor of Science in Economics from the State University of New York, USA. Before joining RSIS, Teck Boon held research positions at both the Lee Kuan Yew School of Public Policy and the Department of Economics, NUS.

PITFALLS OF THE "INTERNET-OF-THINGS"

This article first appeared in RSIS commentary

Authored by
Ton Teck Boon

Synopsis:
The global network of Internet-enabled sensors, devices, and systems called the spheres-of-Things" promises many upsides and put many IoT products vulnerable to hacking. In the IoT age, it is vital to strike a balance between the risks and rewards

Commentary
THE "INTERNET-OF-THINGS" (IoT) is a catchall phrase for the global network of Internet-enabled sensors, devices, and systems that collects and shares a vast amount of personal data. Wildly diverse and growing fast, the billions of IoT products out there right now include fitness trackers, medical devices, household appliances, mobile gadgets, and even Barbie dolls. According to IT research company, Juniper Research, there are now more than 13.4 billion IoT products in use and by 2020, the figure will hit 38.5 billion.

Proponents contend that once we are fully immersed in IoT, the technology will engender myriad benefits. They claim that energy-saving IoT products will enhance our situational awareness and quality of life too through automation. For example, when a sleep tracker is connected to a smart air conditioner and coffeemaker, the wearer not only wakes up to a freshly-brewed cup of coffee but also feels refreshed because the temperature in his bedroom is synced to his sleeping pattern.

So not only does the wearer of the sleep tracker know the quality of his sleep, but he is also doing his part for the environment by letting the smart air conditioner adjust the temperature accordingly throughout the night. As appealing as this high-tech option may sound, it is unfortunately clouded by serious cybersecurity concerns.

The Downsides of IoT
The biggest fear right now is that a large number of IoT products are susceptible to hacking. Indeed, many IoT products are resource-constrained, meaning that they do not come with firewalls, encryption authentication, and antivirus capabilities builtin. We install security protection into our smartphones, PCs, and tablets; but doing so with the smart toothbrush or kettle may not be possible because they have limited computing power. Even if it were possible to patch IoT products with security upgrades after they had left the factory, it would be a logistical nightmare given their sheer numbers out there.

According to estimates from Hewlett Packard, a staggering 70% of IoT products currently in use are vulnerable. In a sign of things to come, penetration tests (or "pentesting") designed to uncover security vulnerabilities in IoT products have shown that it is possible to breach home Wi-Fi networks via IoT appliances. So hackers could in theory exploit weaknesses in everyday IoT products and work their way into corporate or government networks as employees bring their infected gadgets to work.

Sounds incredible but in 2013, we inched closer to this dystopian nightmare when hackers breached the database of Target and stole the credit card numbers of 40 million customers apparently by hacking the US retailer's Internet-enabled heating and air conditioning system.

Implications of a Cyber Takedown
In the worst case, hackers could take over or shut down major infrastructure networks throwing critical sectors like banking, telecommunications and transportation into chaos. The consequences would be catastrophic.

Or they might attempt to retrieve sensitive information stored in these networks. Bear in mind that IoT products collect a vast amount of personal data. Not just plain information like names, birth dates, and contact details but revealing information like energy consumption patterns, geo-location data, and lifestyle habits. To the untrained eye, this kind of information means nothing but in the hands of sophisticated criminals, it can be used to make scams more elaborate and convincing.

The reality is that IoT is a "double-edged sword". Indeed, having a IoT of security cam that lets you see what is happening in your house via your smartphone might make a lot of sense when you are away but it also means that cybercriminals could watch you in your own home if the system had been compromised. Likewise, owning a smart TV that is voice-activated might seem like a nifty idea except that your privacy would vanish if hackers were able to listen in on your private conversations.

Common sense tells us that we should never share anything online that we do not want others to know about. But with the advent of IoT, the datafication of our most intimate personal information is unavoidable; more importantly, we will not have a choice about it. So, if you are concerned about your online data privacy, then you should be very worried about IoT.

It's Not All Bad - And besides Do We have a Choice?

Shunning IoT products completely would be unrealistic since they do bring important benefits. Furthermore, as existing electronic products get phased out, users have no choice but to replace them with IoT ones. Try buying a rear-projection TV today or apply for a job without a smartphone and you will see the impracticality of snubbing the latest technology.

If turning our backs on IoT products is not feasible, then what we need is to prepare for its inevitable arrival. For major organizations, this would mean integrating IoT products in a step-by-step fashion- taking the time to evaluate the technology with great care.

The government can certainly help by assessing every IoT product for potential risks. If a IoT product is deemed too much of a cybersecurity risk then it should not be integrated into a broader network.

The government also needs to set industry standards to ensure that IoT product manufacturers do not cut corners on their products since building in added security features will eat into their bottom line. Apart from tightening security in the cyber domain, the government also needs to put tough data protection measures in place to limit abuses of personal information collected by IoT products. Lastly, consumers play a crucial role too; besides ensuring that their IoT products are secure, they must also be responsible enough to avoid those that are not.

When all is said and done, we need to recognize that at the moment no software based product is really "hacker proof" and sooner or later, some IoT products will be breached by hackers. So some loss of online data privacy is to be expected as we enter the IoT age. The key then is finding that balance between risks and rewards- that sweet spot which allows us to enjoy the upside while keeping the pitfalls to a level that is tolerable.

REBALANCING ENCRYPTED MESSAGING APPS

This article first appeared in RSIS commentary

Authored by
Ton Teck Boon

Synopsis:
End-to-end encryption has made instant messages more secure: But the technology has also made it more difficult for authorities to fight terrorism and crime. Reverting to the previous encryption technology rebalances security requirements with privacy concerns.

Commentary
THE RECENT decision by Brazilian authorities to ban WhatsApp- an instant messaging app used by millions of people worldwide is emblematic of the kind of push around the world to rein in commercial messaging apps featuring state-of-the-art encryption.

In the case of WhatsApp, every message sent is encrypted with a unique "key" typically, a very large number ensuring that only the person(s) holding the specific key can unscramble the message.Even if a message were intercepted during transmission, it would be unreadable without the key. Besides WhatsApp, iMessage, Line, Signal and Telegram are some examples of commercial messaging apps featuring this technology.

To be precise, this form of encryption is called end-to-end encryption (or E2EE, for short). In earlier versions of the technology, the app developer retained the keys, thus making it possible for the developer to unscramble users' encrypted messages under court orders. But with E2EE, the keys are kept in the users' computer or mobile device and as a result, app developers are no longer able to hand over users' encrypted messages even if ordered to. The only way authorities can gain access to users' unscrambled messages in this case is to get physicalaccess to their devices.

Upsetting Balance between Privacy and Security
History-wise, developers began seeing the need for more secure communications after a series of embarrassing photo leaks in 2014 involving quite a few female celebrities. But to be sure, the monetary reward was also a big driver behind the development of encrypted messaging apps since the company that develops the app with the strongest encryption will invariably corner the lion's share of this incredibly lucrative market. The advent of encrypted messaging apps would not have been a problem except that as instant messages became more secure, criminals and militants have also caught on to their usefulness paradoxically exploiting for their benefit the very justification that underpinned these apps in the first place.

Indeed, Islamic State (IS) militants are known to take advantage of these apps for secure communication as well as to reach out to potential recruits around the world. As a case in point, Malaysian authorities arrested three of its citizens earlier this year who were thought to have been recruited by IS through Telegram. IS operatives also claimed responsibility for the recent Jakarta attack using the same messaging app.

But terrorists are not the only ones exploiting encrypted messaging apps; cybercriminals, organized crime, drug dealers, and even child predators use them to mask their illegal activities. Besides making it more difficult to monitor suspects, encrypted messaging apps have also made it harder for law-enforcement agencies to collect evidence against them. If anything, the situation now is akin to the police not being able

to enter a house to collect evidence even with court authorization.

Because encrypted messaging apps have made it significantly more challenging for authorities to disrupt terrorist plots and fight crime, the vital balance between privacy and security has arguably shifted in favor of the former.

Old Way Still the Best Way

One way to restore the current imbalance is to introduce so-called backdoors or hidden flaws into the apps so that authorities might gain access to the plaintext (unencrypted) messages of suspects. The backdoors could be introduced into either the hardware or software granting the authorities unlimited access. But even this strategy is imperfect. Apart from potential abuses, this approach can be downright dangerous since cybercriminals and hostile foreign governments can exploit these bush-in flaws just as well. Once a flaw is intentionally introduced into the system, it is only fair to assume that someone out there would find a way to exploit it for malicious reasons.

Technological advancement occurs at such a brisk pace that it sometimes blinds us to the fact that earlier inventions already held the solution to an existing problem. Indeed, by reverting to the previous encryption technology (in which the keys are retained by the app developer), the authorities can again monitor encrypted instant messages if needed. As in the past, an app developer will act as a check against illegal government surveillance by scrutinizing requests from the authorities for plaintext messages. The most obvious advantage is that authorities will right away regain the ability to monitor suspected militants' encrypted messages.

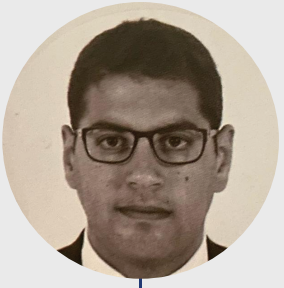
But what is less obvious is that reverting to the previous encryption technology will also serve to push them offline. In the same way Osama bin Laden promptly stopped using his Inmarsat satellite phone when the Al Qaeda leader learned that it was being monitored by US intelligence, the idea here will likewise push militant's offline once they realize that the digital realm is no longer a haven from which to promote violence.

Unlike backdoors, reverting to the previous encryption technology will not lead to a spike in cyber-attacks because the previous encryption technology is sufficiently robust against the majority of cybercriminals. We know this because the authorities had to turn to the app developers for help and if they could not break into the previous encryption technology, then chances are run-of-the-mill hackers would not be able to either. Not all developers are expected to cooperate even though their apps now arguably threaten public safety and interest. But even if some were to, it will reduce the multitude of encrypted messaging apps at the moment and allow authorities to then concentrate their cryptanalytic effort on those that remain unbreakable.

Trump Card: Changing Attitudes towards Privacy

Reverting to the previous encryption technology will entail some risks to privacy, but it is still far superior and more realistic compared to introducing backdoors into every mobile device, computer, and encrypted instant messaging software out there.

More importantly, our readiness today to share much personal information online in exchange for greater convenience and accessibility is indicative of our changing attitude towards the notion of absolute privacy. If anything, the popularity of cloud storage and social media websites these days speak to this shift in mindset. And as militants and criminals of all stripes continue to exploit encrypted messaging apps, reverting to the previous encryption technology will restore the delicate the balance between privacy and security.



Christain Karam

Global Head of Cyber Threat Intelligence
UBS AG

Mr Karam is the Director and Global Head of Cyber Threat Intelligence at UBS where he oversees the bank's threat intelligence service that enables the delivery, consumption, analysis and actioning of cyber threat intelligence from various sources to provide the bank with risk awareness and the operations teams with valuable intelligence to identify threat indicators, tactics, techniques and procedures that inform and enable the timely mitigation and response to threats. Also in his role, Mr Karam conducts security research and excellence activities in thought leadership specifically in the area of security and cybercrime. Prior to joining UBS, Mr Karam was the head of the cyber research laboratory and the lead cyber threat researcher at INTERPOL. Mr Karam developed the activities in the fields of global cyber threat research, future trends analysis, cyber intelligence and R&D within the INTERPOL Global Complex for Innovation (IGCI). Prior to joining INTERPOL, Mr Karam was an independent security researcher, penetration tester, and security consultant for several private sector firms.

Mr Karam's subjects of interest and expertise are threat intelligence, threat research, cybercrime, darknets and underground economy. Mr Karam researches also blockchain technology and cryptocurrencies for potential future threats and abuse around money laundering and criminal activities. Mr. Karam is a member of the INTERPOL Global Cybercrime Experts Group, a member of the BlackHat Review Board, and an accomplished public speaker covering highly rated security conferences, governmental events, and think tank forums.

CYBERCRIME: REDEFINING THE THREAT ACTOR LANDSCAPE

Authored by
Christain Karam

Innovation is the key component that has allowed crime to evolve throughout the ages. Criminals are great innovators at heart and have always developed disruptive technologies, as well as pioneered the discovery of unconventional ways to use new and emerging technologies that can be leveraged for their gain.

Today's criminals understand the importance of changing their behavior and modus operandi while embracing the important technological advancements and the high dependency on the digitization of our world to mark another leap in crime history.

Drug dealers, weapons traffickers, money launderers, fraudsters, and cybercriminals have transformed and bolstered their operations by shifting their ways and their core focus on digital elements that allow them to minimize their efforts but maximize their profits. In this short paper, we will review specifically the evolution of the cybercrime threat actor quadrant as well as organized crime's evolved capabilities.

The Threat Actor Quadrant pre-2013

Threat Actor Quadrant prior to 2013 - Fig. 1

The threat actor quadrant (which excludes insider threat) is a high-level representation of threat actor capabilities mapped by skill level versus quality of intelligence that the threat actor may have access to. Before 2013, threat actors were categorized in 4 quadrants:

Low Skill; Low-Quality Intelligence (LS; LQI)
- In this category, threat actors are politically or ideologically motived. Typical examples of threat actors in this area are tied to hacktivism and terrorism who have been known to use tools that are automated and require little skill or knowledge to operate them.

Their attack tactics would usually revolve around the defacement of public websites and Distributed Denial of Service (DDoS) attacks against entities in orderto protest or to disrupt the availability of services causing significant financial losses to the organization. It is estimated that the cost of a high bandwidth DoS attack againstlarge companies could go up to USD 100,000 per hour.

High Skill; Low-Quality Intelligence (HS; LQ1)
- Lone wolf cybercriminals are extremely skilled individuals that may cause significant damage to their targets, but have little understanding of how to monetize their attacks and maximize profit given the lack of quality intelligence enabling high impact attacks against their victims. Their goal is to raise notoriety and reputation in cybercriminal circles.

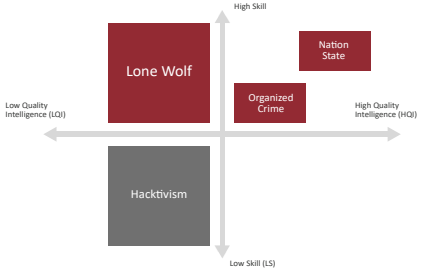
Low Skill; High-Quality Intelligence (LS; HQI)
- Organized crime sees cybercrime as a business problem that needs to be further refined. Organized criminals are financially motived and will

typically buy weaponized and finished malware from developers to use in a carefully built and efficiently run campaign. Their focus will be always on refining the business plan for a higher return on their investment. Before 2013, organized crime groups were slowly maturing their capabilities and skills, what highly characterizes organized crime is their access to high-quality intelligence that allows them to identify important targets and victims. Data theft, extortion, fraud, and carding are some of the numerous modus operandi used by organized crime groups during that period.

High Skill; High-Quality Intelligence (HS; HQ1)

- The cherry on the top. Nation states have it all, skill, resources, and high-quality intelligence. Nation states are the most advanced threat actors in the quadrant and have matured their operations over the past years, mainly focusing on cyber espionage campaigns against political adversaries.

The Threat Actor Quadrant post-2014



Threat Actor Quadrant prior to 2013 - Fig. 1

Post 2013 (Pst Snowden), more attention and research was focused on nation states capabilities. This led to a series of incremental evolutions in the threat actor quadrant most notably in the shift of organized crime in the High Quality Intelligence Quadrant.

Low Skill; Low-Quality Intelligence (LS, LQI)

- No change from a threat actor focus but the commoditization of cybercrime tools allow hacktivists and terrorists to have a larger and more effective arsenal of tools, especially in the DDOS space. First seen in 2016, the Mirai a botnet is seen as a high impact tool that can be rented as a service to inflict significantly damage against target victims. These are still considered the least worrying type of threat actors due to the lack of coordination and the low-quality intelligence but is important not to underestimate the impact that such attacks could have on organizations.

High Skill; Low-Quality Intelligence (HS; LQ)

- Lone wolf cyber criminals were equivariant of freelancers and now have found a permanent or contractual setting with organized crime groups to bolster their capabilities and use their skills in much more elaborate operations that aim to expand threat actor capabilities and impact in the 5th domain.

High Skill; High-Quality Intelligence (HS; HQI)

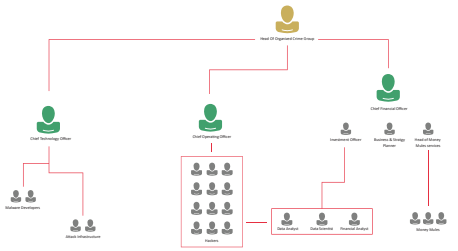
As stated previously, organized crime went through important changes in tactics, operations, and structure.

1) Hiring lone wolf cybercriminals and hackers were done to expand and mature the skill level needed to run operations internally as seen in Fig.2.

2) Studying nation states' tools and capabilities while learning from their operational security planning, structure, and tactics to inspire and uplift the organized crime groups' capabilities. Organized crime did not try to completely replicate the nation states' model, but rather kept evolving key elements to its already existing criminal enterprise model (Fig.3).

It is important to note that organized crime continues to purchase finished malware. Due With the commoditization of cybercrime tools, organized crime continues to invest in such weaponry while delivering attacks in a more targeted, structured, and tactical approach with a clearer goal and motive to its victims.

The criminal enterprise model



Criminal enterprise model in an organized crime group - Fig.3

In the criminal enterprise model, the head of the organized crime group operates similarly to a chief executive officer. This role is supported by 3 officers. A chief technology officer that keeps an oversight on the malware development operations (which organized crime did not focus on before 2013) and the expansion/maintenance of the attack infrastructure. Malware development is key to making sure that the payloads are always updated for a higher and more successful infection rate. The attack infrastructure is very important to maintain and grow to continue generating new attack surfaces against the target victims.

The chief operating officer is in charge of running the active day to day operations of the targeted campaigns that the organized crime group is running against selected victims. Once targets are compromised, the stolen data will be sent laterally to the CFO a function where a group of data analysts, scientists, and financial analysts will examine the data and push recommendations to the CFO and the business planning unit to refocus efforts on a new target that may be of interest or to directly act on financial intelligence that would lead to gain and profit by investing in markets. Information has become for many years now currency 2.0.

No organized crime group would exist without a money mule and cash-out unit. This is a classic unit inherited from the traditional crime models.

That being said, money mule operations have seen a few updates from a modus operandi perspective to incorporate bitcoin (the currency of choice for the past few years in the cybercrime circles) as a main method of payment and cash out.

By maturing this structure, organized crime can bind smart, agile, and effective business strategies for malware campaigns which allows them to maximize their profits. Ransomware is a great case example since it is currently a large global pandemic that was able to exponentially grow its damages and raise considerable profits for cybercriminals due to the ongoing innovation around its business models that have proven to be very successful against its victims.

High Skill; High-Quality Intelligence (HS; HQI)

- Nation states have seen their operations closely monitored by security firms over the past 4 years. This has led nation states to often mimic organized crime or to open source their tools and share them with organized crime groups to blur the attribution process in campaigns that are being tracked globally against them. It is not uncommon to see nation states hiring and recruiting organized crime to operate as a proxy in certain targeted operations. Nation states continue to grow in influence and are the most lethal threat actor group in the quadrant.

In 2006, security researchers were always on the lookout for new malware that had a serious impact on computer systems.

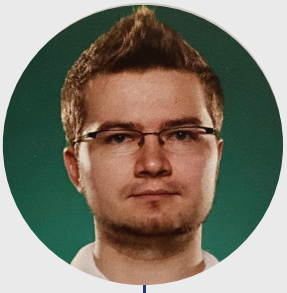
The goal was to always provide an antidote to those anomalies and to stop it from spreading further. This problem was defined back then as trying to find the needle in the haystack. A swift and coordinated response from the industry was always needed to ensure that safety and security online were achievable.

In In 2010, cybercrime operations started using more complex malware and more ingenious business models, therefore researchers had to follow different trails and several different elements of the digital investigation to

identify the full threat picture. This was described as trying to find the needle hidden in many haystacks. Today in 2017, with the complexity of the threat landscape and the threat actors, it is becoming even more difficult to attribute and understand the motives, intent, and real capabilities of the adversaries and cybercriminals.

If one should follow the previous analogies, the problem would be described as finding needles in a stack of needles. Advanced threat actors are mimicking each other relentlessly and are interchangeably using their tools with a common interest of killing the attribution process as much as possible.

It is imperative for law enforcement and the security community to go beyond blocking the attack to identifying and putting the attackers behind bars. It is only then by stopping the fingers operating behind the keyboard, that a real impact can be achieved in securing cyberspace, and that's why a collaborative approach from all industries and authorities is needed to ensure that we can counter such fast evolving and dangerous threats.



Vitaly Kamluk

Director, Global research & Analysis
Team APAC
Kaspersky Lab

Vitaly joined Kaspersky Lab in 2005 as an Infrastructure Services Developer for the Antivirus lab. In 2008, he was appointed to the position of Senior Antivirus Expert before becoming Director of the EEMEA Research Center in 2009. In 2010, Vitaly spent time working in Japan as a Chief Malware Expert, leading a group of local researchers. He specializes in threats focusing on global network infrastructures, malware reverse engineering, and cybercrime investigations.

In 2014 Vitaly moved to the INTERPOL Global Complex for Innovation in Singapore to support the launch of the IGCI's Digital Forensics Laboratory and to provide high-level advice on site. In 2015, Vitaly was appointed to the position of Director of Kaspersi Lab's Global Research and Analysis Team in the Asia Pacific region.

Prior to joining Kaspersky Lab, Vitaly worked as a software developer and system administrator.

Vitaly is a graduate of the Belarussian State University.

ADDRESSING THE CHALLENGES OF CYBERCRIME INVESTIGATION WITH THE HELP OF OPEN SOURCE TOOLS FOR REMOTE FORENSICS

Authored by
Vitaly Kamluk

When investigating cybercrime, access to reliable, robust, flexible as well as userfriendly tools for remote forensics is a must. However, based on the. Experience of our team, in most cases investigators either don't have such tools or only have tools with limited functionality. This significantly extends the length of the investigation and may sometimes even prevent the crime investigators from collecting some crucial evidence. In the latter case, remote locations combined with a lack of time and/or resources can mean that it is not possible to make a trip or hire local experts. Meanwhile, this problem may have a rather simple yet effective solution.

The solution would be a tool that allows a professional digital forensics specialist to connect remotely to a computer that carried relevant forensic images as attachments or even original evidence in the form of hard drives infected with malware, and then collect evidence in a way that would make it admissible in court. To the best of our knowledge, there is no tool commercially available that would allow for the remote acquisition of disk images, or triage, without either tampering with the evidence system or requiring the purchase of some expensive hardware. Perhaps it is widely believed that existing methods of cybercrime investigation work pretty well. But they don't. Here's why.

The challenges of cybercrime investigation on Darknet

Even though in recent years we have seen multiple successful cybercrime investigations, there are obstacles that investigators face on a routine basis. One major challenge is that more and more cybercriminals nowadays use so-called Darknet services to create the backbone infrastructure for a crime.

Darknet services e.g. the Tor protocol, Blockchain-based solutions etc.) All operate in a way that is significantly different from the way "regular" web technologies work. Based on our experience in running cybersecurity and cyber forensics training for law enforcement agencies (LEAs) around the world, the very concept of the Darknetecosystem itself has yet to be fully understood by operatives involved in cybercrime investigation.

Nothing is surprising in this situation: in fact, a full understanding of how Darknet technologies work requires more time and practice than law enforcement agencies are ready to spend, because resources are limited, and cybercrime is only one of many types of crime that modern LEAs have to investigate. In other words, this is a very specific area, which requires a specific set of computer skills.

Another challenge is the fact that a suspect doesn't have a defined geographic location. When it comes to Darknet technologies, the task of identifying a suspect's geolocation becomes significantly harder than in cases where "regular" web technologies are involved. This is due to two main reasons: first, locationobfuscation technologies, like Onion-routing, make it more difficult for law enforcement agencies to identify the source of malicious code and the possible suspect behind it. Second, in many cases, it is just not clear under whose jurisdiction the computer of interest is located and what legal procedures must be followed by an investigator to get access to the evidence.

Both issues are potentially solvable. But to do so in a reasonable amount of time the investigators need to have access to multiple computers involved in cybercrime.

But this is a problem because in most cases today "getting access to evidence" means "go to the exact location and

get physical access to the infected machine". This results in additional travel costs, increased time for the the investigation, the need to address differences in legislation, etc. Investigators have to go to a remote location because even when using most of the existing solutions for forensics, you need a trained forensic specialist in the place of interest to acquire the data and do triage analysis in the proper way. In most of In the cases we have witnessed there were no such specialists available.

A lack of well-trained resources is not only about not having a specialist in a remote location who can set up a Linux system properly. It is potentially a much bigger problem and part of the overall problem of investigating cybercrime on the Darknet. Here's why.

The new kind of investigators

First of all, based on our experience in assisting law enforcement agencies around the world, we can say that modern police officers working on cybercrime investigations come from police academies and schools, not from IT departments at universities. In many cases, cybercrime investigation skills are something they acquire in addition to their main set of skills. Sometimes it is perceived as just another training course that, once completed will raise the professional level of the investigator forever.

Additionally, commercial software businesses, which develop tools for cybercrime investigations, are trying to adjust to this situation and are making tools that are relatively easy to use by a person with mid- to low-level technical skills. This approach can make the process of gathering and analyzing evidence ridiculously simple, down to pushing two buttons: "Acquire" and "Analyze".

That doesn't help when it comes to some custom and sophisticated cyberattacks, where the investigator has to go beyond standard procedure and fully understand what is happening under the hood of the analysis software.

What I mean by this is that existing tools more or less cover the needs of current cybercrime or a regular crime investigator but, based on our analysis of the direction in which the cybercriminal ecosystem is moving, this will not be the case in the future.

Even today criminals and sophisticated cyberespionage actors are using software, encryption protocols, and other components that are not widely used and are not researched well enough to develop a standard forensic tool for all of them. In the future, the situation will become worse, because aver more diverse software will appear and it will be simply impossible to create a plug-and-play product that would allow data from any source to be processed effectively. Or it would cost enormous sums of money to buy and support.

In other words, there should be changes inthe way cybercrime investigators are trained and which tools they use. Today a cybercrime an investigator is capable, on average, of understanding the basic terminology of cybersecurity and cybercrime, and can translate this terminology into the language which will be understood by lawyers, prosecutors, and judges. Most of the technical job of collecting digital evidence is done either by a third-party cybersecurity expert or by a commercial software solution, or both.

Tomorrow this level of skills will not be enough. The cyber-police officer should be familiar with core software principles, such as OS architectures, software frameworks, network protocols, file formats, compression and encryption algorithms and reverse engineering.

Ultimately police officers should be able to code and create their tools, or patch existing ones to suit their needs. Last but not least, cybercrime investigators should have access to tools, which would allow them to work remotely from any location, flexible enough to be useful in the investigation of crimes conducted with any kind of software. And this is where open-source technologies might be of help.

BitScout - the concept of a universal digital forensics tool

BitScout is a set of software based on open source code, which allows for trusted remote digital forensics and the collection of guaranteed untampered evidence. It gives an investigator the ability to conduct remote forensics operations. We created it for internal use while doing a

For example, a forensics investigator using BitScout while having root-level access does not touch the evidence HDD at all. Instead, the investigator accesses the virtual HDD device of interest in a special isolated container where he has virtualized full root access.

This is not a perfect situation, but luckily it can be improved. For example, a forensics investigator using BitScout while having root-level access does not touch the evidence HDD at all. Instead, the investigator accesses the virtual HDD device of interest in a special isolated container where he has virtualized full root access. This feature allows for full spectrum research of the hard drive (including installing additional software from public repositories) and at the same time guarantees that the data on the real hard drive is not modified.

All possible changes made to the virtual HDD will not make it to the evidence hard drive and will be discarded when the system is shut down. Implementing a copy-on-write technique for such virtual HDDs makes this possible. Moreover, certain types of cyber forensics analysis may require modification to the hard drive. This procedure is a must when it comes to the dynamic analysis of the machine under investigation. To reconstruct the malware behavior within a reasonable time it may be mandatory to launch it on the exact system environment it has infected.

This is needed to find out which actions the malware performs, what servers it connects to etc.

WWW.TACAFRICA.ORG