International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5s, January 2019

The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity

Geetha A Rubasundram

Abstract: ***Money Laundering and terrorism funding has been a problem for years, with regulators and investigators facing difficulties in tracing illicit funds due to legislation and privacy issues. Money laundering using the traditional banking network, or through close relationship based transfers such as the "hawala" require complex investigations. The advent of technology-based money such as digital currencies and advancement of other financial technology, and the use of it under untraceable sites (Dark Web), only complicates the whole issue. The typical biased and wrong perception is that technology based crime can only be perpetrated by individuals who are highly skilled. Further consideration should be taken into account differentiating between the perpetrator, victim and the mechanism used, such as Crimeware-as-a-Service. This case study based research analyses the challenges faced by investigators when investigating crimesvia technology driven platforms, which includesthe assessment of the techniques and legal ramifications to investigate and identify the perpetrators.The results reflect key points that need to be taken into account especially when the investigation involves cross-country jurisdictions as well as various legal frameworks.***

Keywords: Dark Web, Deep Web, Money Laundering, Terrorism, Crimeware-as-a-Service, Network Investigative Technique (NIT)

I.INTRODUCTION

The world has grown closer with the use of the Internet and technology. Businesses, infrastructures, individuals and just about anything is linked to the Internet. The average person interacts with the Internet using the "Surface Web", commonly defined to include webpages that are indexed by normal search engines. The Surface Web contains over four billion indexed websites, making up only about 1% of the Internet. The larger part of the Internet is made up of unindexed contents, known as the Deep Web. The furthest corner of the Deep Web is the Dark Web, whichis anonymously hosted, contains intentionally concealed content and accessible using special software and browsers that mask the IP address(Finklea, 2015). The most common tool to navigate the Dark Web is The Onion Router (TOR), a browser that routes Internet traffic through a series of nodes (voluntary host computers on the TOR network). The random movement of data through the different nodes makes it nearly impossible to trace the data back to an Internet user, enabling anonymity and resisting censorship. Not surprisingly, the most common use for websites on TOR hidden services are criminal in nature as technological advances have always been used to the advantage of the criminal fraternity (McCusker, 2006), including drugs, illicit finance and pornography involving violence, children and animals (Alvater, 2016).However, the expectation of anonymity within the Dark Web maybe challenged. In October 2011, the popular hacktivist group, Anonymous via Operation Darknet, brought down Freedom Hosting, a website hosting service with more than 40 child pornography websites. In 2013, the FBI took control of Freedom Hosting, and as part of their investigation, infected the website with a custom malware designed to identify visitors. The growth of the Internet and World-Wide-Web have enabled many criminal groups to conduct illegal activities in cyberspace (Rowland et al, 2014). Internet forums are used a meeting place and market place for cybercriminals, which are so advanced with systems to rank members and products (Leukfeldt et al, 2016). One such example is the Internet Underground, a shadowy conglomeration of cybercriminals that provides a platform to exchange goods and services using digital currency (also known as virtual currency or e-currency), which does not reflect the direct transaction that occurred between the receiver and seller and can be stored in virtual banks internationally, especially in countries with weak cyber laws (Rowland et al, 2014). The fact that it may not reflect the actual parties involved raises a few legal queries, such as the identification of the parties, the trigger and provider etc.

II.RESULTS

One of the more popular e-currency is Bitcoins, which generally operates outside government regulations. The main attraction of Bitcoins, apart from the convenience of its mechanism, is its anonymity for both the cyber buyers and sellers, which provides yet another advantage for criminals and cyber terrorists. A brief history andexplanation of the mechanism of Bitcoins is required to set the pace of the discussion. Introduced in 2008 as a concept and a year later, as an opensource software, Bitcoin payments and transactions do no need any central administrator, and are processed on a peer-to-peer basis. The transactions are recorded in a public ledger (block chain) using the Bitcoinaddresses of the sender and recipient, stored in a wallet containing the individual's private key, a security similar to a password. The address and cryptographic signature is used for verification, however the details of the wallet and private key are not reflected in the public ledger.

Manuscript published on 30 January 2019.
***Correspondence Author(s)**
Geetha A Rubasundram School of Accounting & Finance, Asia Pacific University, Malaysia,

Governments around the world have had mixed reactions to Bitcoins, some have banned it, neutral in some and recognized legal tender in others. In the United States, the Internal Revenue Service considers the Bitcoin as a commodity rather than a currency, even though its status is still questionable (Gad, 2014). This then raises further complexities of whether crimes involving these mechanisms and currencies can be tried via the traditional definitions of money laundering and other Acts or regulations.

Though most countries do have some level of regulation or legislation covering cybercrime, the definition of what constitutes cybercrime has to a certain extent become vague or covers the general confidentiality, integrity or availability (CIA) elements. McCusker (2006) sees cybercrime being described generically, as any malfeasant behavior ranging from spam emails, denial of service (DoS) attacks, malware and botnet infiltration etc, ignoring the range and depth of complexity and seriousness. This once again, raised legal loopholes on one hand, if the modus operandi does not fit within the scope described. Apart from the anonymity mechanism described above, another angle that needs to be revisited is the perceived profile of the cybercriminals. The traditional perception was that only technology savvy individuals could perpetrate cybercrime. However, apart from modern education and easily available tutorials and guides online, the development of online market places have also changed the profile of the perpetrator. Technology savvy operators have created mechanisms such as the Crimeware-as-a Service (CaaS) to cater for the needs of the non-technology savvy criminal. CaaS is a underground market and business providing illegal services to buyers wishing to conduct cybercrimes (such as attacks, infections and money laundering) in an automated manner, including malware rental and other computing and hosting services (Sood and Enbody, 2013). Based on the development above, a particular concern is the increased trend in the deployment of cyber weapons, especially those that target supervisory control and data acquisition (SCADA) systems, used in critical infrastructure assets (Rowland et al, 2014). This risk is further enhanced with the use of social online networks and markets, since criminals with access to above mentioned forums can increase their criminal capabilities within their network relatively quickly (Leukfeldt E et al, 2016). Clear links exist between terrorism financing, money laundering, cybercrime and traditional criminal activity (Irwin and Slay, 2010). McCusker (2006) discusses the same, questioning whether technological advances have merely facilitated the commission of physical crime or whether in fact, they have led to the creation of a new wave of traditional, but virtual organized crime. Once again, this questions' the legal perspective of who exactly is the perpetrator, and how exactly enforcement would create the link between the crime, the criminal and the platform. The mechanisms behind this may create further complexities in investigations, as it is crucial to distinguish between the operator and the main culprit. Legislations and the subsequent determinations of what constitutes a criminal act and the integrity of the evidence plays a significant role in the case. Investigations for cybercrimes arenot the same as investigations for conventional money laundering and terrorism processes, especially when the trails are obscured due to cyber mechanisms.

A. The Mechanisms of the Dark Web, Digital Currencies and Crimeware-As- A-Service

The cybercrime community has evolved to where crimeware (tools and services to carry out or facilitate illegal online activity) can be readily bought, sold, traded, hired, or licensed in online marketplaces to ready buyers. Gad (2014) identified three facilitating technologies in thecrimeware marketplace: anonymous e-currency (eg: Bitcoins), anonymity networks (eg: TOR) and mobile computing technology. Both Bitcoin and TOR provide the highly valued anonymity feature for cybercriminals, providing a potent opportunity and protection for criminal activities, including crimeware marketplaces since it creates challenges for law enforcement agencies to track and prevent misuse (Ablon et al., 2014). As mentioned in the earlier section, the Bitcoin mechanism and information on the public ledger provides limited information that may not be sufficiently helpful to the enforcement team. A consideration would be to focus on "exit points", as eventually a Bitcoin holder would want to exchange the virtual currency into real money or services. Regulations could be imposed on the platform providers with reporting requirements, however, this would obviously ensure that legal virtual currencies or platforms lose their attraction.

Typical crimeware market places have three main actors (include subject-matter experts and administrators, the crimeware vendors (crime-as-a-service providers) and the general members (buyers and observers))and five cybercrime modes of operation (Crimeware-as-a-Service (CaaS), Pay-per-install, Crimeware toolkits, Brokerage and Data Supplier) (Ablon et al, 2014). CaaS has already been discussed in the earlier section. Pay-per-install involves the outsourcing of the malware distribution process, where cybercriminals provide a third party with instructions to infect targets, and the final payment is based on the number of infected targets. Off the shelf crimeware toolkits provide instructions to infect a system and retrieve data from various sources. Some of the vendors provide brokerage services, being trusted intermediaries for a fee. Likewise, cybercrimes focusing on supply of data, use "drop sites" for private information obtained illegally. Similarly, Leukfeldt et al (2016) classified four positions (core members, professional enablers, recruited enablers and money mules) in the financial cybercrime network, regardless of the relationships and functions. Core members are the main perpetrators who direct and coordinate the crimes; Professional Enablers provide services to the criminal networks on their own initiatives; Recruited Enablers provide services to the criminal networks with the encouragement of the core members and Money Mules who are used to interrupt the financial trail that can be traced back to the core members. Thus, it can be seen that the crimeware marketplace is a structured, bustling meeting haven for many criminals, providing flexible options to suit all needs.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This can be misused for the purpose of cyber terrorism and money laundering, where the complexity of the mechanisms may cause issues with the investigations. A similar modus operandi noted in all the above scenarios is the layering of perpetrators and lack of trail, which enhances the anonymity of the entire crime and mechanism. Combining the research of Ablon et al (2014) and Leukfeldt et al (2016) will then further multiply the layers of perpetrators, and enhance the gap between the perpetrators, platform, victim and crime. Even worse, the crime can become international within seconds. An important aspect of both money laundering and terrorism financing detection is to identify the perpetrator(s), (Irwin and Slay, 2010).

B. Cybercrime Legislations impacting Money Laundering and Terrorism Funding

The Internet provides a possible alternative infrastructure for criminal activities, by being largely unregulated, anonymous and without geographical boundaries. Although it is possible to be traced via the unique numeric identifiers, known as the Internet Protocol (IP) addresses, the Internet provides certain information security applications that allow users to conceal the content of the communications and transactions such as encryption and steganography, or by using an anonymizer to use an untraceable IP address. Users may use easily available encryption tools to convert a message into “ciphertext” for secure transmission or embed a message into an image, sound, or other file through a process called “steganography.” This makes it difficult to determine their content, unless in possession of the rightful key to decode encrypted or steganographic files (Hinnen, 2004). Cybercrime legislation is plagued by the lack of geographically based jurisdictional boundaries. The jurisdictional problem of cybercrime manifests itself in three ways: lack of criminal statutes, lack of procedural powers, and lack of enforceable mutual assistance provisions with foreign states. The Council of Europe’s Convention on Cybercrime (CoC) was created to address the jurisdictional issues posed by the evolution of the Internet. Its solution was to harmonise cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cybercriminals. The CoCis a multilateral agreement geared at facilitating international cooperation in the prosecution of cybercriminals (Weber, 2003). Over the years, countries have developed multi-lateral initiatives to develop and implement legal and regulatory controls to prevent money laundering and terrorism funding over the banking networks and other value transfers, such as the “hawala”. As formal financial systems become more regulated and scrutinized, terrorists and money launderers naturally look for alternatives to move resources (Hinnen, 2004). Although there are some researchers that suggest similarities between the characteristics of money laundering and terrorism funding, Hinnen (2004) and Irwin and Slay (2010) disagree as they believe that both these crimes have different goals. Terrorism is not profit motivated, with an ultimate goal to inflict harm and instill terror, with money launderers being oriented towards financial gains. The same research also states that whilst money laundering generally involves financial transactions designed to conceal the illicit origin of funds, terrorism funding may not necessarily be derived from an illegal source, and may be from donations or business proceeds. Terrorists use the Internet as a medium of communication, source funds, and recruit members. This can be via false fronts such as soliciting donations for charity, perpetrate online crimes such as fraud, intellectual property fraud, identity and credit card fraud etc. These illegal proceeds are also used to finance the activities of the group (Hinnen, 2004). The complex mechanisms and the involvement of the many players require clear indications of what constitutes a crime, and if it is categorized appropriately. Cybercrime can have an international impact within seconds, yet depending on the jurisdiction, this may not be criminalized appropriately.

The Co Ccriminalises nine offences in four categories. The first category targets offenses against the confidentiality, integrity and availability of computer data and systems. These include illegal access, illegal interception, data interference, system interference and misuse of devices. The second category is computer related offences, including computer related forgery and fraud. The third category criminalises content related offences including the dissemination of child pornography, racism or xenophobic contents through computer systems. The final category criminalises offences related to the infringement of copyright and related rights (Weber, 2003). The CoC requires member states to establish a minimum set of procedural rules at the national level whereby the appropriate law enforcement authorities have the authority to conduct certain types of investigations specific to computer crime offences. The powers include expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of computer data, real time collection of traffic data and interception of content data. It also provides a jurisdiction based on citizenship so long as the act is punishable by criminal law, even though it may have occurred outside the geographical location of the state. Although the CoC tacitly allows cross border access to stored computer data without the need to request mutual assistance, such investigations are only allowed when access to the data is publicly available (open source) or when the state conducting the search has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. The CoC also ensures an obligation to cooperate amongst its member states, including the collection of electronic evidence whenever it relates to criminal offence(Weber, 2003). In both the USA Patriot Act and the Homeland Security Act, Congress strengthened the statutory penalties for computer crimes.

C. Investigation Techniques and Cases

The investigation techniques and tools used to investigate traditional money laundering and terrorism financing versus a virtual environment is different. Irwin and Slay (2010) differentiate the detection between the traditional and virtual by comparing the lack of controls and reporting procedures such as the Suspicious Transaction Reports available with conventional banking networks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Investigating cases involving the Dark Web and Bitcoins, requires the use of technology and intelligence tools since the flow of information is halted due to the anonymity of transactions and users. It is vital that pattern recognition techniques and suspicious behaviour maps, rule bases and models already are determined and systems designed to automatically detect potential money laundering and terrorist financing activities.Leukfeldt et al (2016) discusses the role of social ties in the origin and growth of the cybercriminal networks. A large number of networks have emerged and grown due the relationships in the offline criminal underworld. Enablers and mules are also often recruited through existing social networks with forums playing a significant role of providing a platform to communicate and collaborate. Sites hosted by law enforcement for the purpose of attracting and gathering information on criminals are called "honey pots". The capture of terrorist officials or infiltration of terrorist compounds is now often accompanied by the discovery of computers that have accessed the Internet. In 2001, the government's use of remote access search techniques, codenamed Magic Lantern become public (Lerner, 2016). In 2002, the FBI renamed it to a "computer and internet protocol address verifier (CIPAV) to identify suspects who disguise their location using proxy servers or anonymity servers like TOR (Lerner, 2016; Finklea, 2015). However, it was used as a prosecutorial tool only in 2007 (Lerner, 2016). Consequently, the tool was used frequently, and was subsequently rebranded asNetwork Investigative Technique (NIT). NIT consists of four components; a generator, an exploit, a payload and a logging server. A generator runs on the hidden service and produces a unique identification (ID) number that is associated with each user of the dark website. The generator then transmits the unique ID, along with the exploit and payload, to each user's own computer. On on the user's computer, the exploit takes control of the TOR browser and executes the payload. The payload then searches the user's computer for those materials authorized in a search warrant. Relevant information would likely include the individual's username, the unique identifying number of the computers network card and the computers name. The payload then sends the identified information to the logging service to create a record of the computer on a separate FBI computer, enabling the payload to capture the public IP address of the user's computer. The FBI can then use the IP addresses to serve a subpoena on the Internet Service Provider (ISP), to obtain the user's name and physical address. Armed with a probable cause that the user accessed illegal content, the FBI is able to obtain a search warrant for the user's computer and would be able to ensure its compatability when the computer is later seized (Alvater, 2016). The FBI relies on two primary methods to implement remote access search tools if the identity of the user is unknown and only the frequented website is known; social engineering attacks and watering hole attacks(Lerner, 2016). Both methods are complexlegally and may be construed asa violation of privacy. The social engineering method was evident in the case of George Cotrel, for his participation in aonline money laundering scheme, using TOR; undercover agents posed as criminals seeking to launder criminal funds subsequently met him in person in Las Vegas prior to charging him with the crime.

The watering hole attack was reflected in the investigation of Playpen. Playpen, a bulletin board website was launched in August 2014 on the Dark Web, with the primary purpose of advertising and distributing child pornography, had almost 215,000 members, more than 117,000 posts and received an average of 11,000 unique visitors a week. The FBI discovered numerous posts featuring extreme child abuse images and advisory services for users to avoid detection online.Between February and March 2015, the FBI ran an operation in an attempt to bring down Playpen. Steven Chase, Playpen's lead administrator and mastermind had made payments to the hosting company. Chase was arrested following a court-authorized search of his home and forensic examination of his computers and devices seized; depicting images of infants and toddlers sexual abuse. Subsequent to Chase arrest, the FBI obtained approval from the federal court to deploy a NIT, and seized the Playpen computer server from its North Carolina web host, and proceeded to run the site from their own servers in Virginia for two weeks. A key question raised here is does this make the FBI a distributor of child porn during the period that it kept the websites running, rather than shutting them down? The FBI deployed their NIT hacking tool, and used a single warrant to uncover 1,300 IP addresses from visitors who accessed these sites, tracing these addresses back to actual individuals, even though the users had used TOR for anonymity. At least 137 cases have been filed in federal court as a result of this investigation. The tool was linked to the forum hyperlink, and not the website's main page. The FBI has used NIT before, but this is the first time that it has been reported that the NIT was able to get around the protections of TOR. When visitors accessed the website, although their traffic might have been encrypted, a Flash application was secretly installed on the user's computer that quietly sent important data about the user straight to the FBI so that it did not pass through the TOR network at all. The NIT was able to capture the actual IP address of the computer, the type of operating system the user's computer was using, the computer's architecture, the computer's host name, the computer's active operating system username and was even able to issue a unique identifier to the user in order to distinguish all data collected from another user's IP address. Even though it sounds like a successful operation, some of the cases were thrown out due to the sensitive technicalities. The "Going Dark" problem reflects the vulnerability of the gap between the court order legal authority and the practical ability of vendors to intercept electronic communications (Caproni, 2011). Federal Rule of Criminal Procedure 41 (Rule 41) restricts a judge from issuing a warrant from outside their district of jurisdiction, with exceptions. Conflicting judicial opinions in the last five years with regards to the remote access search tools have led to changes, with due regards to granting extraterritorial warrants when suspects use anonymisingsoftware's to mask the location of their computers. This is an issue, and requires creativity and technological advancements to identify the true criminals.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The cases charged under Playpen challenged the validity of the search warrant, claiming that its coveragewas too broad and in violation of Rule 41 of the Federal Rules of Criminal Procedure. Rule 41 authorises magistrate judges, with few exceptions, to issue search warrants only in the judge's own judicial district. In the case of Playpen, opponents of the NIT warrant argued that the magistrate judge violated Rule 41 by authorizing a search of any computer that accessed Playpen. The NIT warrant enabled the FBI to deploy its payload to any activating computer and did not specify persons, location or device for the search or seize. It is believed that the FBI also illegally hacked other innocent users of an encrypted web mail service. Subsequently, Rule 41 was amended to permit a magistrate judge to issue a warrant to hack into computers and seize data outside the judge's jurisdiction when the computer's physical location has been concealed through technical means. Even though the method has undoubtedly helped to bring down child pornographers, the American Civil Liberties Union was concerned that the FBI was able to hack into over 1,000 computers with just a single warrant, and believes that Congress and the public should play a role in evaluating whether law enforcement should be allowed to use NITs at all. However the problem is that although the FBI was granted a warrant to hack 300 specific TORMail users, it illegally went beyond the warrant and hacked the email accounts of many other users too even though the affidavits specifically said that the FBI was only allowed to "investigate any user who logs into any of the target accounts by entering a username and password". The defendant's subsequent argument that the search warrant was unconstitutional was rejected. The defense for Jay Michaud who was arrested for child pornography charges, argued that the FBI should reveal the code used for the hack during the legal discovery process which would subsequently identify Michaud to ensure that it did not go beyond the scope of the issued warrant. The FBI refused to disclose the code, and the presiding judge, Judge Robert J Bryan of the US District Court for the Western District of Washington had to exclude the obtained evidence, stating that the prosecution could not keep the tool a secret and at the same time, expect to use the information as evidence at a trial. This is especially so, when considering the "beyond a reasonable doubt" expectation of evidence. Subsequent to this development, the DoJ had requested for the case to be dismissed without prejudice, which could allow the government to bring new charges against the defendant in the future if circumstances change and they could disclose the technicalities of NIT at that point. Another issue with The "Going Dark" problem is its ability to spread internationally within seconds, especially in countries with weak regulations or when a country may not be eager or able to assist in preventing such crimes. This was evident in yet another money laundering case. Liberty Reserve operated one of the world's most widely used digital currency services. Seven of its principals and employees had been indicted for money laundering and operating an unlicensed money transmitting business. Liberty Reserve emerged as one of the principal money transfer agents used extensively by cybercriminals internationally to distribute, store, and launder the proceeds of their illegal activity. Liberty Reserve was the bank of choice for the criminal underworld because its infrastructure enabled cybercriminals to conduct anonymous and untraceable financial transactions. Liberty Reserve supposedly had more than five million users worldwide who transacted more than $6 billion in criminal proceeds, in its own currency, the LR. The founders, Arthur Budovsky and Vladimir Kats were previously indicted in 2006 in New York for operating an illegal digital money transmittal business, Gold Age Inc. Customers could open Gold Age accounts with minimal documentation, the Gold Age purchased digital gold currency through those accounts and the customers could eventually withdraw the money to any part of the world. The key to Liberty Reserves system was that it never actually received the deposits, instead using middlemen who bought the currency in bulk and then sold in smaller amounts. The illegal money exchangers were in countries with weak regulations. Budovsky was arrested in Spain in 2013, and extradited to the United States in 2014, and received a sentence of 20 years imprisonment in 2016.

On 30 November 2016, an international criminal platform known as Avalanche (Crimeware-as-a-Service rental based on cloud) was dismantled, after four years of investigations, involving prosecutors and investigators from thirty countries resulting in the arrest of five individuals, search of thirty-seven premises and seizure of thirty-nine servers. The Avalanche network had allegedly hosted malicious software's and several money-laundering campaigns, known as money mule's campaigns. Apart from ransomware, online banking passwords and other sensitive information stolen from victims malware infected computers was redirected through Avalanche servers, to backend servers controlled by cybercriminals. The originating investigation was from Germany after an encryption ransomware affected and blocked affected users access, with close cooperation with the US, Europol and other regulatory bodies. Investigators analysed over 130 TB of captured data and identified the server structure of the botnet, allowing for the shut-down of thousands of servers and effectively, the collapse of the entire criminal network. Law enforcement had managed to seize, block and sinkhole (i.e. redirect traffic) from infected victim computers to law enforcement controlled servers using a temporary restraining order from Pennsylvania.Since 2009, criminal groups had used Avalanche to spread malware, phishing and spam activities, sending more than a million emails with damaging attachments and links a week to victims. Once infected, the criminals were able to access bank and email passwords, enabling bank transfers from the victims' account to the criminals account using a double fast flux infrastructure. This infrastructure was specifically created to secure the proceeds of the criminal activity, offering enhanced resilience to takedowns and law enforcement action by redistributing the tasks of disrupted components to still active computer servers. Criminals use the double fast-flux (Domain Name System –DNS), a technique used to hide the criminal servers behind a constantly changing network of compromised systems acting as proxies.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The money mule schemes operating over Avalanche involved highly organised networks of "mules" that purchased goods with stolen funds, enabling cyber-criminals to launder the money they acquired through the malware attacks or other illegal means. The international cooperation is one of the key success factors in these investigations. In October 2015, the US Justice Department charged ArditFerizi, a citizen of Kosovo for cyberterrorism and hacking. ArditFerizi was detained in Malaysia, on a U.S. provisional arrest warrant, and was subsequently extradited to US. Ferizi admitted that on or about June 13, 2015, he gained system administrator-level access to a server that hosted the website of a U.S. victim company. The website contained databases with personally identifiable information (PII) belonging to the company's customers, including members of the military and other government personnel. Ferizi subsequently provided the PII belonging to approximately 1,300 U.S. military members and other government personnel to JunaidHussain, a now-deceased ISIL recruiter and attack facilitator. Ferizi and Hussain discussed publishing the PII of those 1,300 victims in a hit list.Ferizi led a group of hackers called Kosova Hackers' Security, which was responsible for compromising private and government websites around the world. He had also been arrested multiple times for cybercrimes in Kosovo, though he was a juvenile and was released almost immediately. Ferizi was sentenced to 20 years in prison in 2016.

III.FINDINGS

The level of crime as well as the balance between security and privacy is complex. Although, the numbers of TOR users have increased, not all are using it for wrongful activities. But, the risk from criminal activities may at times warrant the use of methods such as the NIT to ensure the greater goodness of mankind. However, this is open to debate, and the level of success of each case. International cooperation is necessary, and clear, consistent laws should be in place to prevent the manipulation of legal loopholes. A strong message has been sent out to cybercriminals though, that possible penetration by the regulators can remove the element of security and anonymity that is perceived to be evident via encryption techniques and the Dark Web. International regulators need to firm up regulations, and to push for a further balance of privacy versus security point of view, whilst ensuring corporations, regulatory bodies as well as individuals adhere to the measures in place. However, security protocols need to also be in place to ensure that cyber terrorists and cyber criminals are not able to access the information illegally, neither can insiders who have access to these data be able to manipulate the information for their personal gain. Although the Rule of Law may play a significant role in ensuring the rights of individuals are maintained, the key question to be thrown back to the honest members of the public is which they would prefer "privacy" versus "security", with the full impact of a terrorist attack via the cyber world being made accessible to them.

IV.CONCLUSION

Though it may seem like a perfect solution in a perfect world, changes need to be made to not only cyber laws but also legal frameworks of countries. Likewise, there is a growing trend differentiating the roles of corporations to battle the risk of cybercrime, policy makers and legislators and investigators to prosecute the crime. It may seem easier to segregate, however, an integration may also be needed. Background checks on employees maybe required more stringently, to ensure persons of dubious backgrounds are not hired, firms need to know what are the legal procedures to follow if they suspect wrong doing or possible terrorism based activities within their workforce, and to understand most importantly, that to withhold information to safeguard their reputation may not be the best way forward. The recent worldwide impact of Ransomware should already be a warning to the public, firms and governments that this risk can escalate without warning, within minutes and can be worse with a cyber-terrorist attack on any of the world's public infrastructure. The case of Uber who withheld the ransomware attack information initially should also serve as a reminder to firms on the drawbacks of the fear and shame. Regulators and legislators need to move from the fear of violation of privacy to a strong hold of the expectation of security, especially with the world's move towards financial technology. However, privacy and anonymity needs to have its place in society, within reasonable boundaries. But, the key question we should all ask ourselves would be "Do we really want privacy at the cost of our security?" Money is being laundered daily by the corrupted and the criminals in many ways, causing economic damages by itself. When money laundering is linked with technology and cybercriminals, including cyber terrorist, shouldn't we get the perspective in place, on the exact level of danger we face in the near future.

REFERENCES

1. Ablon, L., Libicki, M. C., &Golay, A. A. 2014. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Report number: RR-610-JNI.Santa Monica, CA: RAND Publications.SEP http://www.rand.org/pubs/research_reports/RR610.html
2. Alvater, BJ (2016), Combating Crime on the Dark Web – How Law Enforcement and Prosecuters are using Cutting Edge Technology to Fight Cybercrime. Prosecuters Centre for Excellence December 2016.
3. Caproni, Valerie (2011), Statement before the House Judiciary Committee, Subcommittee on Crime, Terrrorism and Homeland Security, Washington D.C (FBI Website: last viewed on 3rd March 2017)
4. DoJ (2017a), Playpen : Florida Man Sentenced to Prison for engaging in a Child Exploitation Enterprise (Accessed from https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise on 14th September 2017)
5. DoJ (2017b), Cotrel George (Accessed from https://www.justice.gov/usao-az/pr/dark-web-defendant-sentenced on 14th September 2017)
6. DoJ (2016), United States of America v ArditFerizi (Accessed from https://www.justice.gov/opa/file/896326/download on 8th September 2017)
7. DoJ (2015), Liberty Reserve Indictment (Accessed from https://www.justice.gov/sites/default/files/usaosdny/legacy/2015/03/25/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted_0.pdf on 8th September 2017)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

8. DoJ (2014), Liberty Reserve Press Release (Accessed from https://www.justice.gov/opa/pr/liberty-reserve-founder-extradited-spain on 8th September 2017)
9. Finklea, Kristin (2015), Dark Web, Congressional Research Service
10. Gad, Mahmoud (2014), Crimeware Marketplaces and their Facilitating Technologies, Technology Innovation Management Review November 2014
11. Hinnen, Todd M (2004), The Cyber-front in the War on Terrorism: Curbing terrorist use of the Internet, The Columbia Science and Technology Law Review 2004 Vol V 2004
12. Irwin, Angela S M and Slay, Jill (2010), Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft, Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010.
13. Lerner, Zach (2016), A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, The Yale Journal of Law & Technology Vol 18 (2016)
14. Leukfeldt E, Rutger, Kleemens, Edward R, P Stol, Wouter (2016), Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis, Crime Law and Social Change November 2016
15. McCusker, R. (2006), 'Transnational organisedcyber crime: distinguishing threat from reality', Crime, Law and Social Change, 46 (4-5), pp.257-273
16. Perri, Frank S and Brody, Richard G (2011), The Dark Triad: Organized Crime, Terror and Fraud, Journal of Money Laundering Control January 2011
17. Primavera De Filippi (2014), Bitcoin: a regulatory nightmare to a libertarian dream.. Internet Policy Review, 2014, 3 (2), pp.43. <hal-01026112>
18. Rowland, Jill; Rice, Mason; Shenoi, Sujeet (2014), Whither Cyberpower?, International Journal of Critical Infrastructure Protection June 2014Sood, Aditya K. and Enbody, Richard J. (2013), Crimeware-as-a- service – A survey of commoditized crimeware in the underground market. International Journal of Critical Infrastructure Protection 6 (2013) 28 – 38
19. Weber, Amalie M (2003), The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal, Volume 18, Issue 1, Article 28

AUTHORS PROFILE

Geetha A Rubasundram is working in School of Accounting & Finance, Asia Pacific University, Malaysia,

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)