Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)

Practitioner's insight

Innovations in International Cooperation to Counter Cybercrime:

The Joint Cybercrime Action Taskforce

(J-CAT)

Tuesday Reitano Troels Oerting

Marcena Hunter*

Abstract: Without significant cooperation between nations and the adoption of new strategies, law enforcement will be left behind, fighting 21st century crime with 19th century tools. Cybercrime has challenged policing capacity in unprecedented ways, demanding increasing cooperation between states, and requiring a more effective investigation capacity. The J-CAT is a Member States led initiative facilitated by Europol's Cybercrime Center, EC3. This initiative is the first of its kind, born out of frustration with traditional tools available to law enforcement, the JCAT has illustrated the importance of developing a task force based in a single physical location, governed by a flexible administrative framework, and that elicits the trust of Member States. The JCAT has prioritised joint investigations on some of the most heinous Internet enabled crimes, including online sexual exploitation of minors, vicious botnets and identity theft rings. The result is an effective platform to collaborate across multiple borders and coordinate international investigations with partners, maximising the effectiveness of international joint and coordinated actions against key cyber threats and top targets. This practitioners' note outlines the genesis and operations of the J-CAT, identifying key success strategies, lessons learned and opportunities for the future.

Keywords: Cybercrime – Law Enforcement – International Cooperation – Cyber-Security – Organized Crime

*Tuesday Reitano is the Head of the Secretariat of Geneva-based NGO, the Global Initiative against Transnational Organized Crime and the director of an independent policy and monitoring unit for the EU on counter-terrorism.

Email: Tuesday.Reitano@GlobalInitaitive.net

Troels Oerting has recently stood down as the Director of the Europol's Cybercrime Centre (EC3) and currently serves as a Managing Director at Barclays Plc.

Marcena Hunter is a Senior Research Analyst at the Global Initiative against Transnational Organized Crime.

The European Review of Organised Crime 2(2), 2015, 142-154

ISSN: 2312-1653

Introduction

The Internet has challenged the fundamentals of criminal behaviour, enabling criminals residing in one jurisdiction to perpetuate crimes in another, whilst laundering money in a third. Multiple layers of identity encryption guarantees criminals almost complete anonymity, and virtual currencies similarly permit traceless transactions. Using these technologies, organised crime groups perpetuate a panoply of criminal acts ranging from online sexual exploitation of children, drug trafficking, identity theft and frauds, to providing secure areas where the exchange of criminal services can be transacted.

These criminal innovations have changed the game in regards to law enforcement, institutions designed for national security and thus uniquely bounded within the framework of the state. Consequently, to mount an effective response to an exponentially growing cybercrime industry, it is crucial for law enforcement agencies from around the world to collaborate, share intelligence and align priorities (Europol, 2014d). Thus, after a decade of ad-hoc bilateral cooperation within the framework of regional and international police cooperation structures, the Europol's European Cybercrime Centre (EC3) has facilitated the launch of an unprecedented initiative, the Joint Cybercrime Action Task Force (J-CAT) on 1 September 2014. The J-CAT is the first physical, co-located and standing cybercrime taskforce composed of Cyber Liaison Officers from committed and closely involved Member States, non-EU law enforcement partners and Europol's EC3.

This article, developed by those intimately involved in the initiative's creation and implementation during the pilot phase, outlines the objectives of the initiative, the rationale behind it, and analyses its functioning following its first six months of operation. The J-CAT is an innovation in the law enforcement response to cybercrime, and offers many possible lessons to other practitioners and analysts.

Genesis of the J-CAT: The Need for a Physical Co-location to

Combat a Virtual Crime

The J-CAT was formed out of frustration with traditional bilateral and multi-lateral cooperation, which proved sluggish in the face of cybercriminals' ability to forge transnational alliances, quickly adopt new technologies and adapt to law enforcement efforts. In the European context, traditional cooperation on cybercrime issues tended to drag out over months, not keeping pace with cyber threats. Traditional coordination consisted of law enforcement agencies contacting each other to either provide or request information, conduct analysis, and determine if the agencies had any matching leads. Agencies would also call for meetings where investigators would work together for a day or two. Generally, after either form of cooperation, a few months would pass before agencies would meet to see if any progress had been made or if goals had been achieved. These efforts at coordination were not only slow, but also unsustainable and had little success in stemming the avalanche of cybercrime that law enforcement officials were facing.

Europol Member States and the EC3 acknowledged that they could not continue to work in this fashion, and that a new, highly-cooperative, multi-sectoral and dynamic response was essential to combat cybercrime in Europe, as well as in the rest of the world. It was from this that the J-CAT was born. The aim of J-CAT is to act as an effective platform to collaborate across multiple borders and coordinate international investigations with partners, maximising the effectiveness of international joint and coordinated actions against key cyber threats and top targets (Europol, 2014d).

The J-CAT operations consist of coordinated investigations into the most potent and widespread of cyber threats, including attacks on children, viruses that steal banking logins, and high-profile criminals, such as those dealing in hacker tools and selling personal data on underground forums. The J-CAT gathers data on specific criminal themes, from national repositories, relevant government and private partners, and transforms this raw data into actionable intelligence, and proposes targets and networks for investigations (Europol, 2014d).

The J-CAT comprises of a number of EU Member States: the United Kingdom, Germany, France, Spain, Italy, Austria, the Netherlands and Norway volunteered immediately. In addition, three American agencies were included, as well as Canada, Australia and Colombia (Europol, 2014d). Europol's EC3 serves as the Secretariat of the J-CAT, undertaking a large portion of the J-CAT's work and providing a platform that supports the J-CAT with analysts, equipment, and safe connections, amongst other things. In addition, the J-CAT organises dedicated consultation meetings with key actors in the private sector and the Computer Emergency Response Teams for the EU institutions, bodies and agencies (CERTEU), to obtain their input on cybercrime threats that affect them and society in general (Europol, 2014d).

Somewhat ironically, in designing J-CAT it was recognised that a single, physical space needed to be created to combat cybercrime, a virtual crime. Past efforts were delayed due to the fact that individuals were working in separate offices, more often than not in different countries and

continents. The physical separation stalled information exchange and coordination efforts. To mount a decisive, coordinated response best practices dictated that a task force be assembled in one physical location to improve communication and speed up cooperation and response. As such, member states that wanted to participate were required to physically relocate a liaison officer to the J-CAT headquarters in Europol.

The designation of a single office has quickly delivered results. By having Member States in one location, with access to the majority of their own intelligence and information at their fingertips, in a secure space, and working in parallel and in easy reach of each other, the J-CAT is able to prioritise actions and cases much quicker and get investigations into “top-level criminals” moving far swifter than before (Brewster, 2014). The J-CAT is not a talk shop, but rather an operational entity and the set-up has directly led to the identification of a number of cases and increased arrests in the first few months of existence (Brewster, 2014).

Overcoming Legislative and Bureaucratic Challenges

Due to its multi-jurisdictional nature, legislative frameworks can form a major hurdle to quickly and effectively combatting cybercrime. In addition, bureaucratic processes, which limit entities’ ability to quickly respond and adapt to the criminal landscape, have slowed law enforcement efforts to combat cybercrime. To circumvent legislative and bureaucratic impediments, the J-CAT was established as an EU taskforce rather than a Europol-led initiative. As an EU taskforce, with one lead Member State and a Board, the legal and bureaucratic frameworks governing the J-CAT are much more flexible than if it had been designed as a Europol taskforce. This provides the J-CAT the freedom it requires to quickly respond to and adapt to cybercriminal threats. Each individual investigation is presented as a proposal to the J-CAT board, which then decides which cases to pursue (Brewster, 2014). Once approved, each operational case has a single, dedicated driver country responsible for managing the investigation.

The legal framework governing the J-CAT also enables the task force to work more freely and quickly with Non-Member States. Often the perpetrators of cybercrime are not located within J-CAT member countries and the J-CAT needs to reach out to these countries and invite them into investigations to secure prosecutions. This is especially important as obtaining prosecutions is a major aim, and indicator of success, of the J-CAT. For example, Russia is a known locus of cybercriminal activity (Group-IB, 2014). However, Europol has no operational agreement with Russia and is unlikely to have one in the foreseeable future. As such, if the J-CAT was embedded within the Europol’s framework it would face major legislative obstacles in working with Russia and pursuing cases. However, because the J-CAT is an independent Member States’ initiative, it is able to work with Russia, or other Non-Member States through ad-hoc proxy agreements. When pursuing a case in Russia, the J-CAT designates a sole Member State to act as a proxy and meet with Russia liaisons, and the proxy makes a case for investigation and prosecution on behalf of the

J-CAT. Via the proxy, the J-CAT then hands the case over to Russia, and works with their national law enforcement to conclude the specific case.

Cooperation with Non-Member states is important for sending the message to cybercriminals that the J-CAT can catch them and that cybercrime will not be tolerated.

While the legal framework governing the J-CAT allows the entity a great deal of operational flexibility, it nonetheless receives considerable support from Europol's EC3. The economic power and technology that the EC3 has brought has been a valuable asset in pursuing investigations in Non-Member States. The EC3 has the budget for financing operational meetings and is able to pay for flights for investigators in Non-Member States. For example, when the J-CAT had a meeting in Kiev, Europol's EC3 was able to pay for the J-CAT members to attend, as well as cover the costs of transport for the Ukrainian police to attend.

Strong Beginnings: J-CAT Successes

In its first six months of operations, the J-CAT has registered a number of successes, demonstrating how the J-CAT is an effective mechanism to quickly and decisively combat cybercrime. On last count, the J-CAT had 17 operations underway, in addition to 9 already conducted and successfully concluded. The six-month evaluation report indicates that all Member States and the J-CAT chair fully support the J-CAT and its work and want to make it a permanent task force.

The operational successes of the J-CAT have come as the result of high-level coordination and prioritisation of cybercrime threats. When the J-CAT was first established, the high number and variety of crimes committed in cyberspace, made it essential to convene a task force to assess threats and prioritise responses. The initial assessments identified areas in which "quick wins" could be achieved to demonstrate the potential for efficacy of the J-CAT and garner continued support.

The following are illustrations of successful operations the J-CAT has been involved in, often initiating and coordinating the operation, in its first six months: *Botnet Takedown*: On 24 February 2015 the J-CAT supported and coordinated a joint international operation targeting the Ramnit botnet. The botnet, which had infected 3.2 million computers all around the world, was used by the criminals to gain remote access and control of infected computers, enabling them to steal personal and banking information and disable antivirus protection (Europol, 2015a). The operation involved investigators from various Member States along with partners from Microsoft, Symantec and AnubisNetworks (EUROPOL, 2015a). In addition to being a success itself, the operation was a clear demonstration of the importance of international law enforcement working together with private industry in the fight against cybercrime.

Operation Imperium

Working in close cooperation with the J-CAT, in September 2014 Bulgarian and Spanish authorities dismantled a highly sophisticated and well-organised international criminal network harvesting financial data from ATMs or tampered POS terminals (Europol, 2014b). The action day for Operation Imperium resulted in 31 arrests, the dismantling of eight criminal labs and the seizure of more than 1,000 devices and dozens of forged payment cards (Europol, 2014b). All raids and arrests took place simultaneously and were coordinated with the support of the J-CAT officers (Europol, 2014b). Operation Imperium is an example of the effectiveness of the J-CAT framework and how it is a powerful mechanism in coordinating efforts between EU Member States to protect customers. The operation also demonstrated the unique tools and data sets the J-CAT can provide national law enforcement agencies that they would otherwise not have at their disposal.

Operation Onymous

In November 2014 Operation Onymous, a unified international action coordinated by the J-CAT, brought down several dark markets running as hidden services on the Tor[1] network. The action aimed to stop the sale, distribution and promotion of illegal and harmful items, including weapons and drugs, which were being sold on online dark marketplaces (Europol, 2014e). Operation Onymous resulted in 17 arrests of vendors and administrators and more than 410 hidden services being taken down (Europol, 2014e). Operation Onymous did not just remove these services from the open Internet, but also hit services on the darknet using Tor where, for a long time, criminals have considered themselves beyond reach. The operation proved that criminals operating in this space are neither invisible nor untouchable, which was an important win for the law enforcement community in countering cybercrime threats (Europol, 2014e).

Global Airport Action

In November 2014 the J-CAT coordinated Global Airport Action targeted at criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data. The international operation, coordinated by the J-CAT, was the result of detailed planning between law enforcement, prosecuting and border control agencies, airlines and credit card companies (Europol, 2014a). Over 60 airlines and 45 countries were involved in the activity, in addition to major credit card companies American Express, MasterCard, Visa Inc. and Visa Europe (Europol, 2014a). The International Air Transport Association (IATA) also took part in the action (Europol, 2014a). The operation resulted in the reporting of 281 suspicious transactions and the arrest of 118 individuals (Europol, 2014a). Besides the successful operational outcome, a global alliance of airlines and law enforcement agencies was created who will be working together on an ongoing basis to combat online fraud and crime.

Child Abuse Material

In November 2014 the J-CAT took part in a Victim Identification Taskforce (VIDTF) to harness international cooperation in the fight against online child abuse material (CAM). Experts from various countries and international law enforcement agencies worked on an unprecedented amount of CAM gathered from seizures and, through the pooling of resources were able to select material and establish links that would otherwise not have been possible (Europol, 2015c). The J-CAT added its own intelligence input, giving essential added-value to leads that had been identified (Europol, 2015c). Europol then distributed intelligence packages to the relevant countries on the victims and offenders (Europol, 2015c).

Another illustration of the J-CAT's value in this arena came with the recent arrest of a Romanian man suspected of sexually-abusing his own two-year-old daughter, filming the abuse and posting the CAM online. The case began when the United States National Center for Missing and Exploited Children (NCMEC) received a report of suspected online child sexual abuse (Europol, 2015d). Analysts at the NCMEC reviewed the report and sent the information to its Homeland Security Investigations (HSI) Liaison Office at Europol (Europol, 2015d). HSI special agents then coordinated with the J-CAT who immediately launched an investigation (Europol, 2015d). The J-CAT cross-checked and analysed all the data, and produced an intelligence package for the Romanian authorities who were rapidly involved (Europol, 2015d). The suspected abuser, his victim and their location were soon identified and Romanian law enforcement officers arrested the suspect and the victim—the suspect's own daughter—was safeguarded (Europol, 2015d). Online child sexual exploitation remains one of the most heinous crimes enabled by the Internet, and is thus a priority for law enforcement action.

The Road Forward: Challenges and Opportunities

Cybercrime is an immense threat, severely challenging the international law enforcement community and there is no sign it will subside in the future. Judicial and legislative obstacles and the exponential growth of cybercrime, specifically darknet marketplaces, pose significant challenges, just to name a few hurdles (Europol, 2014f). Looking forward, the J-CAT is acknowledging and addressing these and other challenges, as well as seeking out and utilising new tactics to combat cybercrime.

Specifically examining judicial and legislative obstacles, in general cybercriminals remain out of the judicial reach of the J-CAT Member States. As an illustration, in the operation to arrest the Romanian man abusing his daughter, referred to above, a lack of harmonised legislation on data retention presented issues in the initial stages of the operation. While the J-CAT was able to overcome the hurdle in this particular operation, other states may not be as willing or as capable as Romania to cooperate with the J-CAT operations in the future.

In particular, a lack of cooperation from Russia has proven to be a challenge. The majority of the cybercrime currently seen in Europe is Russian-speaking crime (Europol, 2014f). Though this does not necessarily mean the cybercriminal activity is originating or taking place in the Federation of Russia, if investigations are to succeed and result in prosecutions, there must be action on the Russian side. As the recent investigations into the Cryptolocker and Gameover Zeus malware showed, tracking and arresting Russian cybercriminals has proven tricky and the alleged perpetrator, Evgeniy Bogachev, remains at large despite a global law enforcement effort to apprehend him (Brewster, 2014). To overcome this specific challenge, the JCAT is seeking to form ties with the Eastern Bloc and encourage increased engagement from Russia.

More broadly, there are a number of other countries that also still provide a relatively safe haven to cybercriminals. These may be countries that do not have any cybercrime laws in place, or do not have the expertise and capabilities to deal with online criminals, or where corruption enables online criminals to operate, or indeed where political motives prevent international cooperation from happening (Brewster, 2014). For example, the quickly growing cybercrime phenomenon in West Africa, with cybercriminals taking advantage of weak jurisdictions, is of concern (Europol, 2014f). However, as the J-CAT becomes more established, strengthens its international connections, and broadens its scope of work, it is expected that an increasing number of countries will start to take online crime seriously and become more cooperative, reducing the number of cybercrime “safe havens”.

The anonymity and exponential growth of the crime, specifically dark web market places, also poses a formidable challenge for the foreseeable future. Dark web cybercrime sites proliferate at a rate far greater than law enforcement has been able to take them down. Consequently, it can be difficult to justify the effort and cost of operations aimed at dark web marketplaces, especially when there are so many other forms of cybercrime equally deserving of attention. While the J-CAT cannot match the current proliferation of dark web market places, Operation Onymous, described above, hit at services where cybercriminals have considered themselves beyond reach. As similar operations are repeated in the future, the J-CAT will deliver the clear message that criminals operating in this space are neither invisible nor untouchable, hopefully reducing the growth rate of dark web marketplaces. Although an uphill battle, the threat the dark web poses to nations and populations warrants the effort and cost to continue to pursue cybercriminals operating in this arena.

In regards to future opportunities, the J-CAT is providing a common platform to compile and analyse huge data sets, facilitating coordinated investigations, examining how to build an evaluation and feedback loop with academia, assessing how to integrate prosecutions into investigations and fostering public-private partnerships.

In particular, developing partnerships between law enforcement authorities and the industries that are specifically vulnerable to cybercrime is essential to effectively target cybercriminals. Cooperation between law enforcement and the financial sector has already led to several

operational successes and fruitful preventive action, good examples being Operation Imperium and Global Airport Action.

In recognition of the need to partner with the private sector the J-CAT is continuing to work to establish and strengthen partnerships with private businesses, specifically banks and security vendors. In September 2014 the European Banking Federation (EBF) and EC3 signed a Memorandum of Understanding (MoU) which paved the way for intensifying cooperation between law enforcement and the financial sector in the EU (Europol, 2014c). In addition, in January 2015 the EC3 signed a MoU with AnubisNetworks, a cybersecurity and threat intelligence IT company (Europol, 2015b). Security vendors have contacted the J-CAT and want to provide information and work together in the fight against cybercrime. The MoU with AnubisNetworks is a first step in this regard, creating the possibility to work together through the exchange of expertise, statistics and other strategic information.

In addition, the J-CAT recognises the value of working with academia. The JCAT has reached out to multiple universities in an effort to better analyse information gained from large-scale operations. The J-CAT hopes that by supplying information and data collected from large-scale operations to academics for the purpose of analysis and research, together J-CAT and academia may better understand how cybercrime occurs and develop new techniques for evidence gathering. By focusing on the root of the threat and developing new investigation techniques the J-CAT will be better positioned to overcome the challenges the anonymity of cybercrime poses.

Trust and Cybercrime: An Intractable International Challenge

In developing the J-CAT, in addition to requiring a single, physical space and operational flexibility, it was recognised that establishing and maintaining trust amongst partners while still being able to pursue perpetrators in Non-Member States was of paramount concern. When States do not trust one another they are less inclined to share intelligence, severely handicapping the ability of law enforcement to undertake and pursue investigations. In an irony similar to creating a single, physical space to combat a virtual crime, it is necessary to limit membership to effectively combat an organised crime impacting potentially every country in the world. Consequently, to encourage trust amongst partners, the J-CAT restricted membership to a handful of states, and this has been one driver for the success of the initiative.

The J-CAT Member States have asserted the importance that they place on having a limited membership in order to maintain a robust intelligence exchange. This is a vital prerequisite to achieve the J-CAT’s goal to have real investigations, and not merely scratch the surface of international cybercrime. The value of a small membership group is evidenced by the numerous successes the J-CAT has achieved since its inception. This is not to say the J-CAT will not work with Non-Member States or membership will never be expanded. When investigative leads call for

the cooperation of Non-Member States, they can be brought in temporarily, for specific investigations. While the J-CAT has not excluded the possibility of including additional partners—states such as Japan, some of the Nordic countries, and Belgium have requested to be involved, for example it has been agreed that new members will only be added with the approval of current Member States and if there is full confidence their inclusion will not detract from the strong intelligence exchange currently in place.

In addition to trusting one another, Member States must trust the J-CAT mechanism and process itself. Thus, in its operations the J-CAT governance body and secretariat (Europol) works to ensure that trust is respected and maintained. To encourage Member States to contribute knowledge and trust the J-CAT, no agency shares intelligence directly with other agencies, but rather shares it with the J-CAT. The intelligence is given a handling code by the contributing State dictating to what degree it can be shared. The handling codes encourage states to share intelligence, with the knowledge it will not be used in a manner counter to the State's national interests. The handling codes are:

- H1: For police use only and cannot be used for prosecutions.
- H2: Very sensitive. States maintain ownership of H2 intelligence. The JCAT is allowed access to all H2 intelligence, but cannot reveal it to other countries. This allows J-CAT to identify when there is a hit in multiple states' intelligence and facilitate a bilateral or multilateral dialogue.
- H3: Intelligence is exchanged only between the 8 permanent member states.

Handling intelligence in this manner encourages trust and fosters a dynamic intelligence system. By having access to Member State intelligence, the J-CAT has the ability to advocate countries to lift handling codes or to share intelligence with specific countries.

By contrast to the restricted membership model of the J-CAT, the INTERPOL Digital Crime Centre (DCC) in Singapore demonstrates an alternative structure with a broad membership base. The DCC, which opened in October 2014, is open to all 190 INTERPOL member states. Like the J-CAT, the DCC's objective is to combat cybercrime and, it hosts a digital forensic laboratory to co-ordinate investigations (D'Cruz, 2014) and brings together liaison officers in a physical space. However, due the large membership base, the DDC has not yet been able to create a framework by which members can as easily or directly share information, and thus far, since its inception the DCC has found it is extremely limited in what it has been able to achieve.

Replicating the J-CAT Model

The J-CAT has achieved a number of significant successes during its short time in existence and has proved it is an effective model to combat cybercrime. Consequently, there are calls to replicate

the model, applying the J-CAT framework to combat cybercrime in other regions as well as utilising the model to combat other forms of organised crime.

The J-CAT framework illustrates the importance of designating a single physical location for task force action, as well as limiting the legislative and bureaucratic constraints faced by task forces and the membership base. There is a large number of States seeking membership of the J-CAT. However, as restricting membership remains important within the framework of the J-CAT, other regional bodies may seek to establish similar anti-cybercrime task forces limited to a few key partners. By replicating the J-CAT model other regional bodies are likely to achieve success, especially since they are more likely to be facing similar cyber threats and cybercriminals.

In addition, following the success of the J-CAT, Europol is looking to apply the model to other transnational security challenges. There are discussions on replicating the J-CAT model to address other organised crimes, as well as threats from terrorism and violent extremism. Europol is considering a new initiative that will be aimed at looking at web-pages containing and promoting illegal material and radicalisation. Operations will then work with industry to shut-down the web-pages. Other foreseeable operations will delve more deeply into the terrorist and foreign fighter phenomenon, investigating how they are recruited, how they travel to war zones, and what happens when they get back. With an estimated 5,000 foreign fighters, these questions have been very difficult to investigate, trace and prevent. It is hoped that by applying the J-CAT model, Europol will be better equipped to prevent and combat terrorist threats.

Conclusion

Without significant cooperation between nations and the adoption of new strategies, law enforcement will be left behind, fighting 21st century crime with 19th century tools (Global Initiative Against Transnational Organized Crime, 2015). The J-CAT is proving to be an effective mechanism to combat cybercrime, a global threat truly changing the game in regards to policing. Borne out of frustration with tools available to law enforcement, the J-CAT has illustrated the importance of developing a task force based in a single physical location, governed by a flexible bureaucratic framework, and that elicits the trust of Member States. The result is an effective platform to collaborate across multiple borders and coordinate international investigations with partners, maximising the effectiveness of international joint and coordinated actions against key cyber threats and top targets (Europol, 2014d). In turn, the establishment of the J-CAT is a major step forward in equipping law enforcement with the 21st century tools necessary to fight a 21st century crime, and an initiative worth continued evaluation and possibly replication across a wider range of jurisdictions and crimes.

References

Brewster T (2014) *Europol launches taskforce to fight world's top cybercriminals*.

Available at:

http://www.theguardian.com/technology/2014/sep/01/europol-taskforcecybercrime-hacking-malware [Accessed 7 April 2015].

D'Cruz T (2014) *Interpol opens Singapore center to fight cyber crime*. Available at:

http://www.reuters.com/article/2014/10/02/us-asia-cybersecurityidUSKCN0HR0OG20141002 [Accessed 7 April 2015].

Europol (2014a) 118 *Arrested in Global Action against Online Fraudsters in the Airline Sector*. Available at: https://www.europol.europa.eu/content/118-arrestedglobal-action-against-online-fraudsters-airline-sector

Europol (2014b) 31 *Arrested in Operation against Bulgarian Organised Crime Network*. Available at: https://www.europol.europa.eu/content/31-arrests-operationagainst-bulgarian-organised-crime-network [Accessed 7 April 2015].

Europol (2014c) *European Banks and Europol Join Forces to Fight Cybercrime.* Available at: https://www.europol.europa.eu/content/european-banks-and-europoljoin-forces-fight-cybercrime [Accessed 7 April 2015].

Europol (2014d) *Expert international cybercrime taskforce is launched to tackle online crime*. Available at: https://www.europol.europa.eu/content/expertinternational-cybercrime-taskforce-launched-tackle-online-crime [Accessed 7 April 2015].

Europol (2014e) *Global Action Against Dark Markets on Tor Network*. Available at:

https://www.europol.europa.eu/content/global-action-against-dark-marketstor-network [Accessed 7 April 2015].

Europol (2014f) *The Internet Organised Crime Threat Assessment (iOCTA)*. Available at: https://www.europol.europa.eu/content/internet-organised-crime-threatassesment-iocta [Accessed 7 April 2015].

Europol (2015a) *Botnet Taken Down through International Law Enforcement Cooperation*. Available at: https://www.europol.europa.eu/content/botnettaken-down-through-international-law-enforcement-cooperation [Accessed 7 April 2015].

Europol (2015b) *EC3 and Anubisnetworks Initiatie Cooperation in Fighting Malware Threats*.

Available at: https://www.europol.europa.eu/content/ec3-andanubisnetworks-initiate-cooperation-fighting-malware-threats [Accessed 7 April 2015].

Europol (2015c) *Efforts Stepped-Up to Identify Victims of Child Sexual Abuse*. Available at: https://www.europol.europa.eu/content/efforts-stepped-identify-victimschild-sexual-abuse [Accessed 7 April 2015].

Europol (2015d) I*nternational Police Action Leads to Rescue of 22-Month Old Romanian Sex Abuse Victim.* Available at:

https://www.europol.europa.eu/content/international-police-action-leadsrescue-22-month-old-romanian-sex-abuse-victim [Accessed 7 April 2015].

Group-IB (2014) *High-Tech Crime Trends*. Available at http://report2014.groupib.com/ [Accessed 7 April 2015].

The Global Initiative Against Transnational Organized Crime (2015) *Cybercrime*. Available at: http://www.globalinitiative.net/programs/cybercrime/ [Accessed 7 April 2015].