Thirteenth United Nations Congress on Crime Prevention and Criminal Justice

Doha, 12-19 April 2015

Distr.: General
2 February 2015

Original: English

Item 5 of the provisional agenda[*]
Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime

Workshop 3: Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation[**]

Background paper

Summary

The present background paper provides an overview of common and specific aspects of crime prevention and criminal justice responses to cybercrime and trafficking in cultural property, two prominent examples of evolving forms of crime that have gained increased relevance as a consequence of globalization and the development of information technology. While criminal groups have exploited the opportunities offered by these phenomena, effective measures are needed to increase knowledge of the scale, roots and modi operandi utilized in the commission of related offences, to develop effective prevention strategies, improve the exchange of information and strengthen national frameworks and international cooperation among Member States.

[*] A/CONF.222/1.

[**] The United Nations Secretariat wishes to express its appreciation to the members of the United Nations crime prevention and criminal justice programme network, especially the National Institute of Justice of the United States of America, the International Scientific and Professional Advisory Council, the Korean Institute of Criminology and the European Institute for Crime Prevention and Control, affiliated with the United Nations, for assisting in the preparation and organization of the Workshop.

Contents

I. Introduction

1. During the Asia and Pacific, Western Asian and African regional preparatory meetings for the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, Member States acknowledged the importance of developing a comprehensive response to the evolving crimes of cybercrime and trafficking in cultural property.[1] In the same way as with many other crimes, the foundations of effective prevention strategies and criminal justice measures against those evolving forms of crime are a detailed knowledge base and a clear understanding of criminal facilitators and patterns.

2. In the working paper prepared by the Secretariat on comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime,[2] a multilayered typology of new and emerging forms of crime, based on possible roots and drivers and common modi operandi, was explored. Globalization; the proximity of poverty, conflict and weak rule of law to high-value markets; and the rapid emergence of new forms of modern technology were identified as possible roots and drivers of new forms of crime. The paper further identified changes in the structure of organized criminal groups and the use of corruption to facilitate offences as key modi operandi.

3. Alongside other crime types, such as piracy, abuse and exploitation of children, and trafficking in wild fauna and flora, the offences of trafficking in cultural property and cybercrime are commonly identified as falling within the category of emerging, or evolving, crimes.[3] As discussed in document A/CONF.222/8, such acts may not always be entirely new, but can also represent the re-emergence of "conventional" crime types, or the evolution of new ways and means for the commission of established offences.

4. For example, domestic theft of and trafficking in cultural property have existed for centuries. It is only in the last few decades, however, that the international community has sought to regulate the trade in cultural property and to specifically criminalize the theft of art and antiquities. At the same time, globalization has facilitated the increasing involvement of organized criminal groups, leading to globalized illicit markets in stolen cultural property and the possibility of generating significant profit for organized criminal groups and, possibly, terrorist groups. Similarly, computer-related acts, including unauthorized use of computer systems and the manipulation of electronic data, have been recognized in many countries as criminal offences since the 1960s. It is only with the advent of the Internet, however, that globalized information communications technology has come to be used for committing criminal acts with transnational reach, in the form of contemporary cybercrime.

5. As such, cybercrime and trafficking in cultural property exemplify the potential impact of roots and drivers, such as globalization and the emergence of new forms of technology, on criminal innovation. While the two crime types may

[1] A/CONF.222/RPM.1/1, paras. 33 and 35; A/CONF.222/RPM.2/1, paras. 38 and 40; and A/CONF.222/RPM.4/1, para. 70.

[2] A/CONF.222/8.

[3] See, for example, General Assembly resolution 66/181, para. 18.

differ in various aspects, such as the primary object of the offence, they do share a number of commonalities.

6. Trafficking in cultural property is related to the theft of, trafficking in and sale of tangible objects that have value because of their particular significance to cultural heritage. While the object of cybercrime is often intangible, such as computer data or a computer system, a proportion of cybercrime acts is centred around theft and resale. Computer-related acts for personal or financial gain or harm, for example, may involve the theft of online banking or credit card details and their subsequent resale for use in financial fraud or theft. As with trafficking in cultural property, the seller and buyer may well be located in different jurisdictions.

7. As regards the degree of criminal organization, groups involved in cybercrime may show a relatively fluid structure.[4] There is, however, increasing evidence that traditionally structured hierarchical groups are also making use of the service-based nature of the cybercrime market to carry out more sophisticated crimes.[5] In that respect, the spheres of trafficking in cultural property and of cybercrime can intersect at the level of the illicit sale of cultural objects through the Internet. The International Criminal Police Organization (INTERPOL), the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the International Council of Museums have recognized, for example, that the illicit trade in cultural objects over the Internet is a serious and growing problem, both for countries of origin and destination.[6] The International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences[7] address that problem by recommending the establishment of reporting and monitoring mechanisms specifically on the trade of cultural property through the Internet.[8]

8. In addition to the nature of the crimes themselves and their intersection as described above, commonalities can also exist at the level of crime prevention and information-gathering for criminal justice purposes. There has been a lack of detailed trend and statistical information for both crime types. Until recently, much of what was known about trafficking in cultural property came from case studies of specific forms of the crime, such as art theft or the looting of historical antiquities. However, efforts have been undertaken to strengthen available information, including by collecting police and court statistics on trafficking, theft, possession, handling and unlawful excavation of cultural property through the United Nations Survey of Crime Trends and Operations of Criminal Justice Systems. The results confirm the need for systematic and ongoing data collection, in order to achieve representative conclusions. However, the large number of different acts falling under the general term “cybercrime” also presents a challenge for data collection.

[4] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013, draft), p. 46; and Blythe Bowman Proulx, “Organized criminal involvement in the illicit antiquities trade”, *Trends in Organized Crime*, vol. 14, No. 1 (March 2011).

[5] European Police Office, *The Internet Organised Crime Threat Assessment 2014* (The Hague, 2014), p. 10.

[6] UNESCO, INTERPOL and International Council of Museums, “Basic actions concerning cultural objects being offered for sale over the Internet”. Available from www.unesco.org/new/en/culture/themes/illicit-trafficking-of-cultural-property.

[7] General Assembly resolution 69/196, annex.

[8] Guidelines 3 (d) and 10.

Nonetheless, methodologies involving the use of multiple data sources may offer promising approaches in that respect.

9. While the commission of the offence might occur in a single jurisdiction in both cases, trafficking in cultural property and cybercrime also share the common element of transnationality, rendering international cooperation a key factor in effective responses. The crucial importance of enhancing international cooperation in that respect was highlighted in all the regional preparatory meetings for the Thirteenth Congress.[9] With respect to cybercrime, one estimate suggests that between 30 and 70 per cent of cybercrime acts involve a transnational dimension.[10] Moreover, trafficking in cultural property is a predominantly transnational offence.[11] The investigation of criminal acts involving multiple jurisdictions requires the widest possible scope of mutual legal assistance in investigations, prosecutions and judicial proceedings, with a view to enhancing the effectiveness of and expediting procedures.

10. International cooperation is facilitated where national legal frameworks contain criminalization of the same substantive underlying conduct. In the case of trafficking in cultural property, specific offences may include trafficking, illicit export and import, and theft of cultural property, as well as looting and illicit excavation of archaeological and cultural sites.[12] In the case of cybercrime, specific criminal law provisions are usually required in order to criminalize conduct directed against computer data or systems, such as the offence of illegal access to a computer system or computer data.

11. Finally, responses to both forms of crime are likely to be most effective when they involve a multi-stakeholder approach. A significant proportion of Internet infrastructure, upon which many forms of cybercrime, and trafficking in cultural property, rely, is owned and operated by the private sector. Objects of cultural value may fall under wide ownership, including that of the State, private individuals, museums, trusts and other non-governmental associations. The involvement of all relevant stakeholders, including through public-private partnerships, is critical to raising awareness of crime risk and promoting good crime prevention practice, as well as to facilitating investigations and arranging compensation or restitution for victims.

12. The present background paper aims to build on the framework set out in document A/CONF.222/8, with a view to illustrating lessons learned and approaches to international cooperation for the evolving crime types of cybercrime and trafficking in cultural property. In the paper, the knowledge base for each crime type is examined and challenges and practice in national legislative approaches, modes of investigation and forms of international cooperation are examined. Where appropriate, possible entry points for crime prevention are identified. It considers what action may be taken both by States and by the international community as a

[9] A/CONF.222/RPM.1/1, para. 34; A/CONF.222/RPM.2/1, para. 40; A/CONF.222/RPM.3/1, para. 61; and A/CONF.222/RPM.4/1, para. 71.

[10] UNODC, *Comprehensive Study on Cybercrime*, p. 183.

[11] CTOC/COP/2010/12, para. 33.

[12] See guideline 16 of the International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences.

whole, with a view to strengthening global crime prevention and criminal justice responses.

II. Cybercrime

A. Identifying the challenge

13. In 1994, it was noted in the *United Nations Manual on the Prevention and Control of Computer-related Crime* that "the potential extent of computer crime is as broad as the extent of the international telecommunication systems."[13] While, perhaps unsurprisingly, the word "Internet" was used only once in the Manual and the word "cybercrime" was not used at all, its conclusions carried great foresight. While the focus of the Manual was on the concept of "computer crime", it is well recognized that today's cybercrime indeed relies on globalized information communications technology, in particular the Internet, to commit criminal acts with transnational reach.

14. As terminology has evolved, academic efforts have been undertaken to define the term "cybercrime".[14] A modern approach is to recognize that cybercrime is not necessarily a legal term of art, but rather an aggregate term for a collection of acts committed against or through the use of computer data or systems. Other approaches focus on offences against computer information, or the use of information resources for illegal purposes.[15]

15. Acts that commonly fall under the category "cybercrime" include those in which computer data or systems are the object against which the offence is directed, as well as those in which computer or information systems form an integral part of the modus operandi of the offence. Examples of the former include offences against the confidentiality, integrity and availability of computer data or systems, such as the act of illegal access to computer data or systems (sometimes referred to as "core" cybercrime acts). Examples of the latter include the use of computer data or systems for fraud, theft or causing harm to others, and computer and Internet-content related offences, including hate speech, child pornography, identity-related crime and the online sale of illicit goods.[16]

16. In general terms, however, the boundary between cybercrime and conventional crime is increasingly blurred. As electronic devices and global connectivity become ever more pervasive in daily life, electronic evidence, such as text messages, e-mails, Internet browsing data and social network site data, are becoming standard in many conventional criminal investigations. The digital forensic tools and requests to electronic service providers used in such cases, as well as many of the challenges

[13] *United Nations Manual on the Prevention and Control of Computer-related Crime*, International Review of Criminal Policy, Series M, Nos. 43-44 (United Nations publication, Sales No. E.94.IV.5), para. 12.

[14] See, for example, David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, Polity Press, 2007).

[15] See, for example, the Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences related to computer information (2001).

[16] UNODC, *Comprehensive Study on Cybercrime*, p. 16.

and investigative good practices, are often the same as those used in cybercrime cases. As such, while the present paper focuses on acts commonly considered to constitute cybercrime, many of its points and conclusions have a broader application with respect to electronic evidence in general.

17. A key underlying driver of both contemporary cybercrime and the rise in electronic evidence is the development of global electronic connectivity. Today, there are almost 3 billion Internet users, representing around 40 per cent of the global population. The majority access the Internet through mobile broadband, with mobile broadband penetration at around 32 per cent of the global population; almost four times as high as in 2009.[17] The number of devices connected to Internet Protocol (IP) networks is expected to be almost twice as high as the global population by 2018.[18]

18. While such rapid growth in Internet and computer technology has enabled economic growth and widened access to vital services such as education, health care and e-governance, it has also opened new possibilities for criminal activity. Cybercrime tools such as "botnets" (a term derived from the words "robot" and "network"), for example, may consist of global networks of tens or hundreds of thousands of victim devices, each infected with malware that can be remotely controlled by criminals. Social media sites may be used for criminal harassment, hate speech, threats of violence, extortion or dissemination of private information belonging to individuals, on a global scale within a matter of seconds. As criminals seek to also target the Internet of things, so the global potential for criminal activity may further increase.

19. In addition to the global nature of the challenge, the last decade has also seen cycles in the degree of anonymization offered by the Internet, and its resulting use in criminal acts. In its early days, the Internet was widely assumed to be largely anonymous, at least insofar as users did not understand the technical possibilities for tracing online activity back to individuals. In recent years, however, criminal justice systems have grown more accustomed to the concepts of IP addresses and connection logs and to the use of court orders to obtain data from electronic service providers. As a result, the electronic traces left by Internet users have become increasingly accessible to investigators, although obtaining Internet data may require significant time and effort. Equally, advances in digital forensic tools, including "plug-and-play" forensic devices that are simple to use, have facilitated the routine analysis of data stored in digital devices such as computers and smartphones.

20. Technology is continuously progressing, and the forensic tools and cybercrime investigative approaches of today are facing challenges that could not have been foreseen a decade ago. Free and widely accessible software, for example, offers 256-bit encryption of individual files or of whole data storage devices. Without a password, or key, data encrypted in that way is practically inaccessible to law enforcement agencies. The even more advanced 2,048-bit encryption represents, to date, a theoretically unbreakable standard. New, decentralized anonymizing

[17] International Telecommunication Union, "The World in 2014: ICT facts and figures" (Geneva, 2014).

[18] Cisco, "The zettabyte era: trends and analysis", Cisco Visual Networking Index (San Jose, California, 2014).

networks, often referred to as the “dark web”, operate alongside the conventional Internet. Services such as the Onion Router (Tor) make it extremely difficult for many law enforcement authorities to determine the origin of electronic communications, or the identity of “hidden service” websites. Such hidden services can be used to anonymously host illicit online markets for drugs, weapons or child pornography. Some of those networks also offer the possibility of decentralized, encrypted data storage in participating network “nodes”. Electronic documents or images stored in that way are, again, practically inaccessible to law enforcement agencies. The implications of such technologies for law enforcement agencies are profound and raise the question of how law enforcement responses can best keep pace with the rate of cybercrime innovation.

B. Measuring cybercrime

21. One approach to the measurement of new forms and dimensions of crime, including cybercrime, requires a combination of measures, such as information on perpetrators, information on flows within illicit markets and information on numbers of criminal events, harms and losses and resulting illicit financial flows. For cybercrime, a number of data sources can be used in that respect. They include police-recorded crime statistics, population-based and business surveys, victim reporting initiatives and technology-based cybersecurity information. Additional sources also include techniques such as URL crawling and “botnet” takeover.

22. Although police-recorded cybercrime statistics should not be disregarded, it is clear that they have significant limitations, as most victimization is not reported to the police. In one survey of 20,000 Internet users in 24 countries, only 21 per cent of respondents who said that they had been a victim of cybercrime reported the act to the police.[19] Globally, law enforcement agencies may use different statistical methodologies and approaches, making international comparisons difficult. In addition, the overall level of police-recorded cybercrime acts is strongly associated with the number of specialized police, suggesting that statistics can be indicative of police investigative activity rather than underlying cybercrime victimization.[20]

23. Population-based victimization surveys of individuals and businesses offer an important alternative source of information. Surveys suggest that, for the general population, cybercrime victimization is significantly higher than for “conventional” crime forms. Victimization rates for online credit card fraud, identify theft, responding to a phishing attempt and experiencing unauthorized access to an e-mail account vary between 1 and 17 per cent of the online population for 21 countries across the world, compared with typical burglary, robbery and car theft rates of under 5 per cent for the same countries.[21] Private sector enterprises also report similar victimization rates. In Europe, for example, enterprises report victimization rates of between 2 and 16 per cent for acts such as data breach due to intrusion or

[19] Symantec, “Norton Cybercrime Report”, 2012. Available at http://us.norton.com/cybercrimereport.

[20] UNODC, *Comprehensive Study on Cybercrime*, annex 2.

[21] Survey data provided by Symantec.

phishing.[22] One study found that, in 2012, identity fraud victims increased by more than 1 million, with perpetrators stealing more than $21 billion, the highest amount since 2009, although significantly lower than the estimated $47 billion loss in 2004.[23]

24. Survey-based data that include information on financial loss resulting from cybercrime can be used to construct estimates of the impact of cybercrime. In one survey, consumer victims in 24 countries across the world reported average direct losses of between 50 and 850 dollars as a result of cybercrime incidents experienced in one year.[24] Using data from a number of surveys, a further study estimated that the global direct, indirect and defence costs of a number of forms of cybercrime, including online banking fraud, online payment card fraud and advance-free fraud, amounted to hundreds, if not thousands, of millions of dollars per year.[25]

25. Analysis of cybercrime markets also offers possibilities for estimating the nature and extent of some forms of cybercrime. One such approach focuses on the analysis of online forums that function as criminal "social networks" for the sale and purchase of social goods and the sharing of criminal information.

26. One 2011 study made use of available data from six underground web-based forums, containing over 2,500,000 posts and 900,000 private messages from over 100,000 users. Among the most commonly traded merchandise were credit cards, bank account details and tools used in the commission of fraud.[26] Recent analysis of threads from 13 web forums suggests that lists of stolen credit card details are offered online for an average price of around $100, and criminal tools such as credit card skimmers can be purchased for an average of $2,400.[27] New research technologies also offer the possibility of web-crawling of Tor hidden services. That can facilitate the systematic identification and categorization of the number and type of dark-web sites related to topics such as illicit drug sales, child pornography, sale of weapons or cybercrime tools.[28]

27. Finally, characterization of perpetrators assists in understanding the nature and modus operandi of underlying criminal organizations. It is likely that there is no standard "profile" in that respect. A comparatively small number of highly skilled programmers and hackers may drive cybercrime innovation and offer their skills as a criminal service. The ready availability of exploit and malware kits, however,

[22] Eurostat, Information society statistics, Community survey on ICT usage and e-commerce in enterprises, 2011. Available at http://ec.europa.eu/eurostat/web/information-society/data/database.

[23] Javelin Strategy and Research, "2013 Identity Fraud Report: Data Breaches becoming a treasure trove for fraudsters". Available at www.javelinstrategy.com/brochure/276.

[24] Survey data provided by Symantec.

[25] Ross Anderson and others, "Measuring the cost of cybercrime", in *The Economics of Information Security and Privacy*, Rainer Böhme, ed. (Springer Berlin Heidelberg, Berlin, 2013).

[26] Marti Motoyama and others, "An analysis of underground forums", in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2011).

[27] Thomas Holt and Olga Smirnova, "Examining the structure, organization, and processes of the international market for stolen data", research paper prepared for the National Institute of Justice, Rockville, Maryland, United States of America, March 2014.

[28] Martijn Spitters and others, "Towards a comprehensive insight into the thematic organization of the ToR hidden services", paper presented at the IEEE Joint Intelligence and Security Informatics Conference, The Hague, September 2014.

means that many perpetrators no longer require advanced knowledge. Increasingly, forms of cybercrime may also require large numbers of low-level “foot soldiers”. In one recent pre-paid debit card fraud scheme, an organized criminal group recruited hundreds of people in 26 countries, resulting in over 40,000 simultaneous cash machine withdrawals on two separate occasions. An estimated $45 million was stolen.[29] Although more than 80 per cent of cybercrime acts may originate in organized crime,[30] it is clear that the wide typology of group structure, including loose criminal associations, presents a challenge to any straightforward characterization of cybercrime perpetrators.

C. Preventing and combating cybercrime

28. Information on the nature and extent of cybercrime is an important component in the design of effective prevention and investigation strategies. Awareness-raising strategies designed to prevent online consumer fraud, for example, may require a different approach to awareness-raising in the area of online child protection. In that respect, at the Asia and Pacific, Western Asian and African regional preparatory meetings for the Thirteenth Congress, the development of tools and programmes that could facilitate cybercrime awareness and prevention was recommended. Information on cybercrime threats and trends can also inform investigative responses. The investigation of online illicit drug sales, for example, requires skills and techniques different to those used in the forensic examination of computer devices. While available data on cybercrime can help focus efforts in order to respond to emerging trends, the range of possible cybercrime acts requires that countries develop capacity across a broad range of prevention and investigative responses.

29. In addition to cybercrime measurement capacity, national responses to cybercrime have to be taken within the areas of legislation and policy frameworks, including criminalization and procedural powers; law enforcement and criminal justice capacity for cybercrime investigation, digital forensics and the handling of electronic evidence; mechanisms for international cooperation in criminal matters; and cybercrime prevention.

30. National cybercrime policies, strategies and legislation are an important starting point in setting the framework and priorities for responses to cybercrime. The UNODC online cybercrime repository (to be launched in 2015) will contain details of national strategies identified in some 50 countries, covering areas such as cybercrime awareness-raising, international cooperation, law enforcement capacity, legislation, prevention and public-private partnerships. National cybercrime legislation also frequently covers a number of areas, including criminalization, investigative powers, jurisdiction, electronic evidence and international cooperation. Review of national cybercrime laws shows that cybercrime is criminalized through a combination of cyber-specific and general offences. “Core” cybercrime acts such as illegal access to computer data and systems may be criminalized through a

[29] INTERPOL, “Criminal network involved in payment card fraud dismantled with INTERPOL support”, 30 April 2014. Available at www.interpol.int/News-and-media/News/2014/N2014-074.

[30] BAE Systems Detica and the John Grieve Centre for Policing and Community Safety, *Organised Crime in the Digital Age* (London Metropolitan University, 2012).

specific legal provision, whereas computer-related acts for personal or financial gain or harm may be more commonly criminalized through general (non-computer specific) offences.[31]

31. In some cases, national legal frameworks are enacted pursuant to, or are inspired by, multilateral instruments, which may be either binding or non-binding. Such instruments include the African Union Convention on Cybersecurity and Personal Data Protection; the Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences related to computer information; the Council of Europe Convention on Cybercrime; Directive 2013/40/EU of the European Parliament and of the Council, on attacks against information systems; the League of Arab States Convention on Combating Information Technology Offences; and the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security. As regards possible further development of multilateral frameworks, the African Regional Preparatory Meeting for the Thirteenth Congress recommended that States consider the development of a convention on cybercrime in the context of the Thirteenth Congress.

32. In addition to provisions related to criminalization and procedural powers, existing instruments can also contain mechanisms for international cooperation in the cross-border investigation and prosecution of cybercrime. That area represents an increasing challenge for law enforcement authorities. The advent of cloud computing and peer-to-peer data-sharing and storage means that, while the location of specific computer data may be theoretically identifiable at a particular point in time, the data can exist in multiple copies, can be distributed across multiple devices and locations and may be moved to another geographical location in a matter of seconds.

33. Some data storage providers, such as private sector electronic service or cloud providers, may be legally obliged to retain copies of data for a certain time, and will usually release data to law enforcement authorities following a court order or other appropriate legal process. Where the service provider or data are outside of the investigating jurisdiction, however, such legal process often involves the use of formal, and lengthy, mutual legal assistance procedures between States. In the case of other modes of data storage, such as by individuals in a peer-to-peer computer network, data can be difficult to identify in the first place and are often stored in an encrypted manner. Coercive measures against the individual may be required in order to secure and release the data.

34. Discussion at the international level concerning the current, largely territorially based, paradigm for transnational cybercrime investigations and access to data is ongoing at a number of levels.[32] Some existing multilateral instruments establish mechanisms that are aimed at facilitating access to data for law

[31] UNODC, *Comprehensive Study on Cybercrime*, p. 78.

[32] See, for example, Council of Europe, "Cybercrime Convention Committee assessment report: the mutual legal assistance provisions of the Budapest Convention on Cybercrime", document T-CY(2013)17rev, and "Transborder access to data and jurisdiction: options for further action by the Cybercrime Convention Committee", document T-CY(2014)16, and Albert Rees, "International cooperation in cybercrime investigations", presentation prepared for the Organization of American States Regional Cyber Crime Workshop, April 2007.

enforcement agencies, such as points of contact that are available around the clock in cybercrime investigations, expedited preservation of data, transborder access to stored computer data with consent or where publicly available and urgent requests for mutual assistance. In practice, it is clear that even with such mechanisms, many law enforcement authorities face significant challenges in obtaining timely access to extraterritorial data during cybercrime investigations. At the same time, human rights, rule of law and privacy safeguards must be sufficient to ensure that access to data by law enforcement agencies is defined, predictable, proportionate and subject to adequate oversight.

35. Innovations such as the inclusion of a digital evidence module in the redevelopment of the United Nations Office on Drugs and Crime (UNODC) Mutual Legal Assistance Request Writer Tool may assist in streamlining mutual legal assistance processes that concern electronic evidence. In parallel, however, law enforcement may increasingly need to find pioneering ways of collaborating on transnational cybercrime investigations. The involvement of entities such as the INTERPOL Global Complex for Innovation and the European Police Office (Europol) European Cybercrime Centre (EC3) in coordinating and supporting transnational investigations, including by facilitating information-sharing between national law enforcement authorities, may prove especially important in that regard. Other forums and initiatives, such as the Global Conference on Cyberspace, have also offered the opportunity for countries to consider innovative responses in the area of international cooperation against cybercrime.

36. Partnerships for preventing and combating cybercrime, whether at the multilateral or national levels, must also include the private sector. Internet service providers and hosting providers can play a key role in cybercrime prevention. They may retain logs that can be used to investigate criminal activity, help customers in adopting safe online practices and in identifying compromised computers, block some kinds of malicious content and, in general, support a secure communications environment for customers. A number of models exist for public-private partnerships, such as those between law enforcement authorities and electronic service providers. Many are based on information-sharing on the basis of clear rules, trust, restricted membership and the encouragement of mutual benefits and responsiveness. In some cases, industry membership bodies, such as the Cyber Security Research Alliance, offer platforms for the engagement of industry with Governments in the areas of cybersecurity and cybercrime.

37. Finally, capacity-building at the level of national law enforcement and criminal justice systems is critical. While the majority of countries have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence, in many countries those structures are underfunded and suffer from a lack of capacity. As digital evidence becomes increasingly pervasive in the investigation of “conventional” crime, so law enforcement authorities may need to make clear distinctions between, and establish clear workflows for, cybercrime investigators and digital forensic laboratory capacity. Front-line law enforcement officers may also increasingly need to acquire and deploy basic skills, such as those used to produce a sound forensic image of an electronic storage device.

38. As new technological developments such as anonymizing networks, high-grade encryption and virtual currencies become commonplace in cybercrime

offences, investigators will also have to adopt new strategies. Law enforcement authorities may, for example, look to strengthen partnerships with academic research groups that focus on the development of technical methodologies in areas such as the characterization and investigation of virtual currency transactions.[33] Investigators may also need to consider how special investigative techniques, such as surveillance, undercover operations, using informants and controlled delivery in the case of the sale of illicit goods online, may be used alongside Internet investigation and digital forensic techniques. Overall, it is clear that capacity-building for law enforcement and criminal justice actors on combating cybercrime will be an ongoing and continuous process, as technology and criminal innovations continue at a rapid pace.

III. Trafficking in cultural property

A. Identifying the challenge

39. The protection of cultural property is considered one of the biggest challenges for contemporary criminal justice policies. Cultural property has come to be perceived not only as an asset for “source countries”, but also for the whole of mankind, and it deserves to be protected and preserved, for greater historical knowledge, for its contribution to the shaping of cultural identity and its role in social practices. Hence the growing attention that the United Nations and many other international organizations have dedicated to the phenomenon, and the commitment of States to develop and implement international legal instruments aimed at protecting cultural property.

40. The defining conduct that could be related to trafficking in cultural property may be more straightforward than for cybercrime offences, but significant challenges exist in researching the scope and scale of the issue. Those challenges are relevant to the investigation of many types of organized crime and include the complexity of illegal operations, insufficient capacity and awareness among law enforcement agencies, and corruption. Moreover, the proximity of illegal activities related to the export of stolen cultural property to elements of the legal market of arts and antiquities and its methods of operation in many countries demands additional efforts. The difficulties are exacerbated when it comes to cultural property trafficked from illicit excavations in archaeological sites, as it can be enormously challenging to identify the place of origin of archaeological objects.

41. Efforts have been undertaken to collect data on trafficking in cultural property and to identify the methods used by criminal groups. For example, a 2009 study used data from the World Integrated Trade Solution database of the World Bank, which includes data on items over 100 years old, to develop empirical models explaining the smuggling of art and antiquities.[34] The study indicated the existence

[33] See, for example, Sarah Meiklejohn and others, “A fistful of bitcoins: characterizing payments among men with no names”, in *Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2013).

[34] Raymond Fisman and Shang-Jin Wei, “The Smuggling of Art, and the Art of Smuggling: Uncovering the Illicit Trade in Cultural Property and Antiques”, *American Economic Journal: Applied Economics*, vol. 1, No. 3 (July 2009), pp. 82-96.

of a strong link between corruption and the likelihood of underreporting of exports of antiquities, a strong indicator of smuggling.

42. Another approach has been to focus on mapping and measuring illicit markets for cultural property. Some studies have examined the demand side of the markets by focusing on the sale of art and antiquities in auction houses and attempting to establish the source and ownership history of those pieces. For example, a 2002 study focused on over 18,000 pieces of Greek pottery sold in auction houses in the United States of America and the United Kingdom of Great Britain and Northern Ireland between 1954 and 1998 and found that between 80 and 90 per cent of the pieces had no provenance (i.e., the chain of legitimate ownership could not be traced back to the original find).[35] The lack of provenance is not in and of itself an evidence of smuggling, but it represents a significant risk factor. Other studies of illicit markets focus on the supply, most often through the examination and documentation of looted archaeological sites. Some of those studies follow traditional methodologies of social and behavioural science, including field research aimed at documenting the state of archaeological sites in specific countries. More recently, the use of high-powered commercial satellites has allowed for more frequent and expansive surveys of sites for signs of looting. For example, a series of studies in 2008 used digital imagery to document the extent of looting of Iraqi archaeological sites.[36]

43. Some studies have also looked at the different stages of the illicit supply chain of trafficked cultural property. Some have focused on those who loot archaeological sites, such as a 2005 study of 400 such individuals in Belize, which concluded that the main motivator for those perpetrators was economic subsistence, rather than malevolent intent.[37] Another study of looting in Iraq in 2003 and 2004 found similar economic motivation for looting, but also noted the presence of more organized forms of crime, with the control of access to the sites and the murder of Iraqi customs officials trying to combat the looting.[38] A more recent empirical study of a statue trafficking network used oral history interviews conducted during ethnographic criminology fieldwork in Cambodia and Thailand and covered the levels of organization of related illicit activities.[39]

44. Some studies have debated the involvement of organized or transnational organized crime in the illicit markets for cultural property. One study conducted a meta-analysis of previously published studies of trafficking in cultural property and concluded that mapping how the trade occurs and identifying the roles and relationships of different perpetrators in each network is a better approach than

[35] Vinnie Nørskov, *Greek Vases in New Contexts* (Aarhus, Denmark, Aarhus University Press, 2002).

[36] See Elizabeth Stone, "Patterns of looting in southern Iraq", *Antiquity*, vol. 82, No. 315 (March 2008), pp. 125-138.

[37] David Matsuda, "Subsistence Diggers", in *Who Owns the Past? Cultural Policy, Cultural Property, and the Law*, Kate Fitz Gibbon, ed. (New Brunswick, New Jersey, Rutgers University Press, 2005), pp. 255-268.

[38] Joanne Farchakh-Bajjaly, "Who are the Looters at Archaeological Sites in Iraq?", in *Antiquities Under Siege: Cultural Heritage Protection After the Iraq War*, Lawrence Rothfield, ed. (Washington, D.C., AltaMira Press, 2008), pp. 49-56.

[39] Simon Mackenzie and Tess Davis, "Temple looting in Cambodia: anatomy of a statue trafficking network", *British Journal of Criminology*, vol. 54, No. 5 (September 2014), pp. 722-740.

assuming that all types of trafficking in cultural property fit the category of organized crime.[40] Another study applied the network paradigm to explain a relatively flexible structure of the illicit trade in cultural property, and encouraged further studies on the organizational structure of that type of trafficking.[41] Another one mapped the chain of co-perpetrators in a case study of trafficking in cultural property, identifying their role, interrelations and partly hierarchically structured conduct.[42]

B. Responses to trafficking in cultural property

45. Several international instruments have been adopted to respond to trafficking in cultural property. The prevention and sanctioning of harms inflicted on cultural property during wars was the first aim pursued through the Convention for the Protection of Cultural Property in the Event of Armed Conflict and its additional protocols. Other international instruments address illicit imports, exports and transfers of ownership of cultural property under any kind of circumstance. Such instruments include the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property and the Convention on Stolen or Illegally Exported Cultural Objects. The international commitment to the safeguarding of cultural heritage is also found in instruments such as the Convention on the Protection of the Underwater Cultural Heritage. At the regional level, the European Convention on Offences relating to Cultural Property was opened for signature in 1985, but has not yet entered into force.

46. One of the “soft law” instruments of interest in a criminal law context is the model treaty for the prevention of crimes that infringe on the cultural heritage of peoples in the form of movable property.[43] Some of the provisions of that model treaty may provide a basis for normative provisions on combating trafficking in cultural property. In its resolution 2003/29, the Economic and Social Council encouraged Member States to consider the model treaty, where appropriate and in accordance with national law, when concluding relevant agreements with other States.[44]

47. Nowadays the pervasiveness of trafficking in cultural property and its complex features are increasingly acknowledged at both the international and national levels. Trafficking in cultural property and related offences are believed to be a constantly

[40] Jessica Dietzler, “On ‘organized crime’ in the illicit antiquities trade: moving beyond the definitional debate”, *Trends in Organized Crime*, vol. 16, No. 3 (September 2013), pp. 329-342.

[41] Peter B. Campbell, “The illicit antiquities trade as a transnational criminal network: characterizing and anticipating trafficking of cultural heritage”, *International Journal of Cultural Property*, vol. 20, No. 2 (May 2013), pp. 113-153.

[42] Mackenzie and Davis, “Temple looting in Cambodia: anatomy of a statue trafficking network”.

[43] *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: report prepared by the Secretariat* (United Nations publication, Sales No. E.91.IV.2), chap. I, sect. B.1, annex.

[44] See also guideline 14 of the International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences. It should also be noted that the General Assembly, in its resolution 68/186, requested UNODC to continue its review of the model treaty, taking into account the views and comments expressed by Member States, and requested Member States and relevant international organizations that had not yet done so to submit to the Secretariat their comments on the model treaty.

growing sector of criminality, and an increasingly attractive one for national and transnational criminal organizations. Those factors led Member States to negotiate and adopt another “soft law” instrument, the International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences, as a useful framework to guide Member States in the development and strengthening of their criminal justice policies, strategies, legislation and cooperation mechanisms in the area of protection against trafficking in cultural property and other related offences.

48. Since 2000, intergovernmental bodies have expressed growing concern about trafficking in cultural property. Upon adopting the United Nations Convention against Transnational Organized Crime, the General Assembly, in the preamble of its resolution 55/25, declared its strong conviction that the Organized Crime Convention would constitute an effective tool and the necessary legal framework for international cooperation in combating, inter alia, offences against cultural heritage.[45]

49. Subsequently, the Economic and Social Council, in its resolutions 2004/34 and 2008/23, expressed alarm at the involvement of organized criminal groups in trafficking in stolen cultural property, and affirmed the necessity of international cooperation to combat such trafficking. In its resolution 2010/19, the Economic and Social Council considered that the Organized Crime Convention and the United Nations Convention against Corruption should be fully used for the purpose of strengthening the fight against trafficking in cultural property, including by exploring other possible normative developments, when appropriate. At its fifth session in 2010, the Conference of the Parties to the Organized Crime Convention adopted resolution 5/7, in which it urged States parties to use the Convention for broad cooperation in preventing and combating criminal offences against cultural property, especially in returning such proceeds of crime or property to their legitimate owners, in accordance with article 14, paragraph 2, of the Convention. Furthermore, the General Assembly, in its resolutions 66/180 and 68/186, invited Member States to consider, as appropriate, reviewing their legal frameworks, with a view to providing the most extensive international cooperation possible to fully address the issue of trafficking in cultural property, and also invited them to make trafficking in cultural property, including stealing and looting at archaeological and other cultural sites, a serious crime, as defined in article 2 of the Organized Crime Convention, with a view to fully utilizing that Convention for the purpose of extensive international cooperation in fighting all forms and aspects of trafficking in cultural property and related offences. Pursuant to those resolutions, Member States developed the above-mentioned International Guidelines.

50. The International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences contain chapters on the following subjects: (a) crime prevention strategies (covering information and data collection, the role of cultural institutions and the private sector, the monitoring of the market for cultural property, imports and exports and archaeological sites, and education and public awareness); (b) criminal justice policies (covering adherence to and implementation of relevant international

[45] Document CTOC/COP/2010/12 contains an analysis of the elements related to the applicability of the Convention in that field.

treaties, the criminalization of specific harmful conduct or the establishment of administrative offences, corporate liability, seizure and confiscation and investigative measures); (c) international cooperation (including matters related to jurisdictional basis, extradition, seizure and confiscation, cooperation among law enforcement and investigating authorities, and the return, restitution or repatriation of cultural property); and (d) the scope of application of the guidelines to any situation, including exceptional circumstances, that foster trafficking in cultural property and related offences.

51. Responses to trafficking in cultural property broadly depend on inter-State cooperation and coordination and public-private partnerships. Such cooperation and partnerships may cover, for example, the inclusion of comprehensive information into inventories and databases, which may be important tools for exercising due diligence on provenance before a cultural artefact is sold on the legitimate market, including in auction houses, and for assisting in investigations of potential theft and trafficking. In addition to the establishment of national inventories and databases, the INTERPOL database on stolen works of art[46] combines the specific description and pictures of around 43,000 items, which may be particularly helpful in transnational cases. The 13 "red lists"[47] already issued by the International Council of Museums, an international non-governmental organization, classify endangered categories of archaeological objects or works of art in the most vulnerable areas of the world, such as Afghanistan, Haiti and the Syrian Arab Republic, in order to prevent them from being sold or illegally exported. The Art Loss Register[48] is a large private database of lost and stolen art, antiques and collectables. It also contains details of works that have not been stolen, which may provide a deterrent effect to potential thieves and help in the recovery of items[49] in the event of their theft.

52. The importance of a coordinated response is further illustrated by the awareness-raising joint initiative of UNODC, the United Nations World Tourism Organization and UNESCO urging travellers to support the fight against a number of forms of trafficking, including trafficking in cultural property.[50] Another useful example of important cooperation between intergovernmental organizations, national agencies and the private sector is the establishment by the International Council of Museums of the International Observatory on Illicit Traffic in Cultural

[46] Available at www.interpol.int/Crime-areas/Works-of-art/Database.

[47] Available at http://icom.museum/programmes/fighting-illicit-traffic/red-list.

[48] Available at www.artloss.com/en.

[49] It should be noted that article 5 (b) of the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property contains a requirement for States parties to establish and keep up to date, on the basis of a national inventory of protected property, a list of important public and private cultural property whose export would constitute an appreciable impoverishment of the national cultural heritage. Also as a preventive measure, guideline 1 of the International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences states that "States should consider establishing and developing inventories or databases, as appropriate, of cultural property for the purpose of protection against its trafficking. The absence of registration of cultural property in such inventories shall by no means exclude it from protection."

[50] More information is available at www.bearesponsibletraveller.org.

Goods,[51] a collaborative platform that offers information and resources to concerned individuals and organizations.

IV. Conclusions and recommendations

53. Although cybercrime and trafficking may differ in terms of the primary object of the offence, it is clear that new underlying drivers, including globalization and the advent of new technologies, are central to the emergence of illicit markets within each field. As such roots and drivers develop, so can the potential for both crime types to expand and cause increasing loss and damage. In particular with respect to cybercrime, the possible size of the criminal market — in areas such as online extortion, online illicit sales and data breach and sale — is expanding, as an ever greater proportion of the global population becomes connected to the Internet. Anticipating and preparing for the future evolution of illicit markets in the areas of cybercrime and trafficking in cultural property are critical to the design of effective responses.

54. The process must start with systematic research and the development of timely, reliable and accessible statistics on both crime types. As noted in the report of the Independent Expert Advisory Group on a Data Revolution for Sustainable Development,[52] a “global consensus on data” is needed in which technology and innovation can be shared and used for the common good, including through a global network of data innovation. That applies equally to our understanding and measurement of emerging global crime challenges such as cybercrime and trafficking in cultural property.

55. Further action to respond to cybercrime and trafficking in cultural property may include the following:

(a) Member States may consider strengthening their capacity to keep records of related offences and exchanging information at the regional and international levels about the involvement of organized criminal groups, the modi operandi of such groups and the techniques utilized in the identification of forms of cybercrime and trafficking in cultural property;

(b) The interaction between private sector enterprises, whether Internet service providers, banks, global logistics and delivery enterprises, museums or auction houses, or public institutions, such as law enforcement and criminal justice actors, should be pursued through public-private partnerships, in which trust and two-way dialogues can be fostered. More broadly, State regulatory responses that go beyond criminal law and provide incentives for the active involvement of the private sector in crime prevention may be useful in creating an environment that is sensitive to emerging threats and conducive to detecting and countering them;

(c) Member States may consider reviewing and strengthening their national frameworks to prevent and combat trafficking in cultural property, including in circumstances in which cultural property may be particularly vulnerable to trafficking, for example by making use of the International Guidelines for Crime

[51] Available at http://obs-traffic.museum.

[52] *A World that Counts: Mobilising the Data Revolution for Sustainable Development* (November 2014). Available at www.undatarevolution.org.

Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences. In the area of cybercrime, Member States may consider ensuring a balanced legal approach that makes use of specific offences for the criminalization of core acts against the confidentiality, integrity and availability of computer data and computer systems, while reviewing the applicability of other general offences, such as theft, fraud, forgery and personal harm offences, to acts committed online;

(d) Member States may need to examine ways and means of fostering international cooperation in criminal matters. In the area of cybercrime, that may involve, in particular, examining possibilities to expedite formal mutual legal assistance processes and strengthening law enforcement cooperation, and continuing multilateral dialogue in the area of transnational access to computer data. In the area of trafficking in cultural property, that may require increased focus on investigating and prosecuting criminal networks, through the exchange of information among specialized national investigative bodies;

(e) Research and statistics, public-private partnerships, legislative frameworks and international cooperation mechanisms must be underpinned by effective capacity at the national level. Technical assistance and cooperation are important to enable the sharing of good investigative practices, experience and the dissemination of new techniques. In the area of cybercrime, Member States may wish to enhance the sharing of new approaches for the investigation of complex, Internet-based financial fraud, online drug trafficking or the use of virtual currencies for money-laundering, enabling law enforcement authorities in multiple countries to rapidly acquire the necessary skills to counter emerging threats. With respect to trafficking in cultural property, Member States may wish to enhance the ability of border and customs services to identify trafficked cultural property, explore the relations between national frameworks to counter money-laundering and trafficking in cultural property, and to identify and exchange good practices in all areas of crime prevention and criminal justice responses to trafficking in cultural property;

(f) UNODC should continue to offer technical assistance to Member States that is aimed at strengthening crime prevention and criminal justice responses to new and emerging forms of crime, including cybercrime and trafficking in cultural property and related offences, upon request and in coordination with relevant international organizations. Member States may wish to consider, as a matter of priority, making funding available for that purpose;

(g) Member States may wish to adopt, when addressing cybercrime and trafficking in cultural property, a holistic approach that takes into account both current modi operandi and crime threats and possible future evolutions of crime. Responses will need to be increasingly founded on global cooperation, the involvement of multiple stakeholders and the use of technology, such as databases and secure communications platforms.