Exploring the Relationship Between IT Development, Poverty and Cybercrime: An Armenia Case Study

Tim Hall

Department of Policing. Criminology and Forensics

University of Winchester

tim.hall@winchester.ac.uk

Ulrike Ziemer

Department of Social Sciences

University of Winchester

ulrike.ziemer@winchester.ac.uk

Exploring the Relationship Between IT Development, Poverty and Cybercrime: An Armenia Case Study

Abstract

This paper explores the relationship between IT development, regional poverty, and cybercrime, through the case of Armenia. Armenia was selected as it is a former Soviet state that has sought to promote the development of its IT sector in recent years, which has occurred within a context of widespread regional poverty. The paper acknowledges the potentially cyber-criminogenic interactions between developed socio-technological and impoverished legitimate economic conditions, that the literature has noted in several high cybercrime nations. It then examines the case of Armenia by exploring potentially cyber-criminogenic conditions there and by constructing an overview of economic cybercrime trends in Armenia since 2010.. The paper finds that, despite the promotion of IT development within the context of regional poverty, cybercrime in Armenia remains low. It explores, through a series of expert interviews, characteristics of the IT sector in Armenia that have mitigated against the cyber-criminogenic interactions between these two conditions. Finally, it identifies potentially transferable policy lessons, wider theoretical implications, and avenues of future research that emerge from this case.

Keywords: Cybercrime; Armenia; IT development; Poverty; Policy

Exploring the Relationship Between IT Development, Poverty and Cybercrime: An Armenia Case Study

Introduction

It is axiomatic that cyberthreats of various kinds, including cyberwarfare, cyberterrorism, the spread of misinformation online, and economically motivated cybercrimes, have become issues of growing international concern. Despite their potentially 'placeless' qualities, these threats, which can, in theory, originate from anywhere in the world with a connection to the internet, display distinctive geographies that are rooted within specific regions (Hall et al. 2021). The literature of economically motivated cybercrime, for example, despite the challenges of collecting robust data on its origins, associates it with nations such as those of Eastern Europe and the former Soviet Union, Brazil, and Nigeria (Ibrahim, 2016a; Lusthaus, Bruce and Phair, 2020; Lusthaus and Varese, 2017; Whitty, 2018: 109).

This paper explores the relationship between IT development, regional poverty, and cybercrime, through the case of Armenia. Armenia was selected as it is a former Soviet state that has sought to promote the development of its IT sector in recent years (Avetisyan, 2022). This has occurred within a context of widespread regional poverty (Mkrtichyan, Vermishyan and Balasanyan, 2016; Sargsyan and Cairns, 2019; World Bank, 2015; 2020). As subsequent discussions show, this is a combination that is potentially cyber-criminogenic. Armenia has also been identified within one statistical study (Kigerl 2016a: 167) as a phishing specialist nation alongside other widely acknowledged high cybercrime countries such as Brazil, Romania and Turkey. Furthermore, no substantive analysis of cybercrime in Armenia has been undertaken to date.

The paper has four primary aims. First, it establishes the extent to which Armenia can be said to possess a cyber-criminogenic environment. Second, it reviews cases of and recent trends in cybercrime in Armenia in an attempt to establish the nature, types and extent of cybercrime originating there. Third, it explores the interaction between IT development and regional poverty in Armenia, and its relationship to levels of cybercrime. Finally, it identifies potentially transferable policy lessons, wider theoretical implications, and avenues of future research that emerge from this case.

This case study focuses specifically on economic cybercrime and draws on systematic reviews of salient academic, media and grey literatures, statistical sources, and expert perceptions obtained from interviews with researchers based in both Armenia and beyond

with regionally-specific specialisms in socio-economic conditions affecting young people, political science and international relations and online harms, and practitioners from Armenia and beyond from the Anti-Cybercrime Unit of the Armenian police, the CyberEast Project of the Council of Europe, the Internet Society of Armenia, the Atlantic Council's Digital Forensics Research Lab, and from within the Armenian IT sector.

Literature Review: The Uneven Geographies of Cybercrime

Various explanations for the uneven geography of cybercrime have been advanced across multidisciplinary literatures, comprising statistics (Kigerl, 2012; 2016a; 2016b; Mezzour et al., 2014), international relations and political economy (Kshetri, 2010; 2013a; 2013b), criminology and ethnography (Burrell, 2008; Ibrahim, 2016a; Leukfeldt, 2014; Leukfeldt et al., 2017; Lusthaus and Varese, 2017; Okeshola and Adeta, 2013) and investigative journalism (Glenny, 2008; 2011). Despite their diversity, these explanations share a fundamental belief that the geographies of cybercrime are the product of the spatial co-presence of combinations of potentially cyber-criminogenic conditions, which occur only in certain regions. Within this explanation particular significance is attached to the co-presence of developed socio-technological and impoverished legitimate economic conditions in high cybercrime nations.

A variety of potentially cyber-criminogenic conditions have been highlighted across the various cybercrime literatures identified above. Technological, economic, and institutional variables have been the most widely deployed within statistical studies of cybercrime, reflecting the difficulties of operationalising alternative social and cultural variables statistically. Variables deployed here include measures of unemployment, internet use, cybercrime legislation and policy, IT infrastructure and corruption (Kigerl, 2012; Mezzour et al., 2014). These statistical literatures have, generally, embraced a more restricted set of potentially cyber-criminogenic variables than those of other salient literatures. Further, a perennial challenge facing this research is obtaining robust data for the locations of cybercriminals, given the measures they undertake to disguise this (Kigerl, 2016b: 67).

The international relations and political economy literature offers broad surveys of cybercrime, typically for nations widely perceived as major cybercrime threat nations such as China and Russia (Kshetri, 2013a; 2013b) or for large groups of nations, such as the developing world (Kshetri, 2010). They draw largely upon secondary sources and explore the causes and nature of cybercrime from different regions, the ways in which cybercrime and

cybersecurity shapes the relationships between nations, and national and regional responses to cybercrime. They also include comparative discussions of cybercrime from different regions. A major contribution of this literature to cybercrime scholarship is that it recognises a wider range of potentially cyber-criminogenic factors than those highlighted in the statistical literature. Specifically, it also talks about the social legitimacy that cybercrime apparently enjoys in some regions and the potential influence of strongly nationalist political contexts on cybercrime activity (Kshetri, 2010; 2013a; 2013b).

Criminological and ethnographic studies of cybercrime explore the grounded interactions between cybercriminals within their regional contexts (Lusthaus and Varese, 2017). These studies are typically conducted at the micro-scale and employ ethnographic, interview, survey and archival methods. A major contribution of this literature is that it, again, recognises an expanded range of potentially cyber-criminogenic conditions. For example, it discusses poor, limited, or compromised law enforcement capacity, the presence of organised criminal groups within cybercrime economies, the influence of materialistic cultures and cybercriminals' deployment of various historical narratives, such as histories of colonial and corporate exploitation, to justify their own targeting of external victims (Adeniran, 2011; Armstrong, 2011; Burrell, 2008; Ibrahim, 2016a; Okeshola and Adeta, 2013; Olayemi, 2014; Tade, 2013; Tade and Ibrahim, 2011; Warner, 2011).

Within the potentially cyber-criminogenic conditions identified above, the interactions between developed socio-technological conditions and impoverished legitimate economic conditions have emerged as of particular significance to understanding cybercrime development. For example, the statistical literature suggests that the most significant predictors of cybercrime activity within nations are GDP and internet users per capita, where high cybercrime nations tend to be characterised by IT literate populations, as suggested by higher rates of internet users per capita, in regional contexts where they are faced with limited opportunities to deploy their skills within the legitimate economy, as suggested by lower levels of GDP or high rates of unemployment (Kigerl, 2012). Cybercrime's criminological and ethnographic literature also attributes causality to the co-presence of Soviet technological legacies and regional poverty. For example, Lusthaus and Varese (2017: 1), argue that the high levels of cybercrime observed in Romania result from the scientific legacies of the Soviet era, high levels of poverty within the region and extensive corruption. Further, from the international relations and political economy literature Kshetri argues:

> "The combination of over-educated and under-employed computer experts has made Russia and other Eastern European countries fertile ground for hackers. In these economies the growth rate of IT industries is far from enough to absorb the IT workforce" (2010: 1071).

It is not difficult to imagine Armenia's policy of IT development, enacted in the context of ongoing regional poverty, potentially, unwittingly replicating the situation observed by Kshetri in Russia.

Drawing upon this literature, then, we might recognise three potential scenarios stemming from the presence of widespread IT access and usage within the context of regional poverty, whether this be the product of a historical legacy, as in the case of Romania (Lusthais and Varese, 2017: 1) or contemporary cultural and educational preferences, as in the case of Nigeria (Adeniran, 2011) or policy initiatives, as in the case of Armenia, with regard to levels of cybercrime. First, IT skills and infrastructure development are not accompanied by sufficient IT jobs growth, in the context of a cyber-criminogenic environment. Thisresults in a rise in cybercrime as young people with IT-skills fail to access appropriate employment in the legitimate IT sector and seek alternative opportunities in cybercrime. Second, IT skills and infrastructure development are accompanied by sufficient IT jobs growth. This sees IT related economic development with no resultant rise in cybercrime, as young people with IT-skills successfully access appropriate employment in the legitimate IT sector. Third, IT skills and infrastructure development are accompanied by sufficient IT jobs growth. This sees IT related economic development with an accompanying fall in cybercrime, or slowing of cybercrime growth, as young people with IT-skills successfully access appropriate employment in the legitimate IT sector and those involved in cybercrime recognise opportunities to deploy their skills in the legitimate IT sector and some abandon cybercrime in favour of legitimate alternatives.

The first of the three scenarios above, reflects situations that have been observed in some confirmed high cybercrime nations in Eastern Europe and the former Soviet Union and Nigeria (Kshetri 2010: 1071; Kigerl, 2012: 482; Lusthaus and Varese, 2017: 1). We are yet, though, to see a literature that connects IT development, poverty and cybercrime that explicitly recognises instances of IT development in the context of regional poverty, with no rise in cybercrime, or that speaks of the potentials of IT development in such contexts to reduce cybercrime or slow its growth. It is lacuna such as these that this paper recognises and aims to begin to address.

Over the past two decades, the Armenian government has considered the IT sector as a strategic path for the development of the country's economy (Avetisyan, 2022). Prioritising the development of the IT sector is linked to existing geopolitical challenges, such as closed borders and unresolved territorial conflicts, as well as some well-established technological traditions originating from Soviet times. During the Soviet era, Armenia was considered a centre for technological research and production, most of which was conducted at the Yerevan Computer Research and Development Institute (Mergelyan Institute). Between 1958 and 1965, the Yerevan Computer Research and Development Institute, created the Razdan family of general purpose digital computers. In addition, the Institute also produced automatic control systems for civil and defence purposes (Tosunyan, 2021). Between 1960-1980, other Soviet Armenian factories Armelectro Factory, Electron and HrazdanMash began to make early computers, automated control systems, radio electronics, space communication devices, rocket launchers, and various parts used in military submarines and ships. The technology sector generally experienced a rather difficult transition period in 1991-1997, when regional conflicts, a declining economy and the emigration of high-level professionals significantly hampered the overall recovery of the economy. In 1998, there were about 35 to 40 programming companies and Internet providers in Armenia, employing, approximately 1000 specialists (Parsyan 2021).

In December 2000, the Government of the Republic of Armenia officially recognized the IT sector as one of the priority sectors for Armenia's economic development (Parsyan 2021). In 2001, the Information Technologies Development Support Council (ITDSC) was established, acting as a liaison hub for the promotion and development of the IT sector between the Government and IT businesses, educational institutions, NGOs, donors and international organizations. In 2019, the new Ministry of High-Tech Industry was established replacing the Ministry of Transport, Communication and Information Technology. The aims of this new Ministry are to create and strengthen conditions for the balanced and sustainable development of high technologies, digitalization, cyber security, innovative technologies, communication, mail, Internet, the spheres of air and space, as well as create and strengthen conditions for ensuring the state's economic growth (Parsyan 2021). Noteworthy here is that most IT companies, almost 95 percent, were founded between 2000-2018 (Parsyan 2021).

While the IT sector is an economically thriving sector, Armenia generally struggles from low levels of cultivation of arable land, limited resources and low growth potential due to political instability and significant geopolitical challenges. Most recently, the 44-day armed conflict

with Azerbaijan over the Nagorno-Karabakh enclave in 2020 and the Covid-19 pandemic reduced growth to a negative rate of 7.6 GDP in 2020, reflecting the reliance on remittances (mainly from Russia and the US) (LloydsBankTrade, 2022). Accordingly, in 2020, the GDP of the IT sector also declined to 5.1 percent (Parysan 2021). In few of these geopolitical challenges, IT development has always been perceived as a way forward in dealing with such economic and geopolitical challenges as it is an industry not dependent on borders (Richard Giragosian, June 2019).

In the space of just over 15 years, the IT sector grew more than 15-fold in the number of firms, 10-fold in number of employees, and total industry revenue now represents 5 percent of GDP, and 11 percent of exports for Armenia (Kassarjian, 2017). The Enterprise Incubator Foundation, a technology business incubator and IT development agency based in Yerevan, reports that the industry's total revenue, which consists of the software and services sector and the Internet service provider sector, reached 922.3 million USD in 2018, a 20.5 percent increase from 2017 (Mkrtumuan, 2019a). The revenue generated in this sector represents 7.4 percent of Armenia's GDP (12.4 billion USD) in 2018 (Ibid.) In comparison, agriculture represents 11.2 percent of GDP and employs 24 percent of the total workforce (LloydsBankTrade, 2022).

Figure 1: The share of the IT sector in the GDP of the Republic of Armenia in 2010-2020 (Adopted from Parsyan 2021).

Research Methodology

The method underpinning this research had two phases. The first gathered empirical information about potentially cyber-criminogenic conditions in Armenia and about cybercrime there since 2010. The issues of availability and validity of empirical information about cybercrime origins is well documented (Kigerl, 2016b: 67). There is, for example, currently no official or comprehensive 'off the shelf' data about the nature and extent of cybercrime from and in Armenia that we could draw upon. This necessitated producing our own overview based on multiple, publicly available sources. This involved a systematic review of relevant academic and grey literatures and statistical and media sources. This was conducted between October 2020 and February 2021 and yielded over 200 items. These were scrutinised and salient empirical information extracted and recorded.

The sources drawn upon through this process included local, national and international media outlets, and independent, international investigative media platforms such as the Institute for War and Peace Reporting and the Organized Crime and Corruption Reporting Project; reports from think tanks and independent non-profit organisations including Carnegie Europe, Chatham House, and Transparency International; internal official sources including items from the Government of Armenia and the Investigative Committee of the Republic of Armenia; items from international organisations and institutions such as the Council of Europe, the European Bank for Reconstruction and Development, the International Monetary Fund, the United Nations and the World Bank; a research organisation, the Caucasus Research Resources Centre; a European Union funded project, EU4Digital and cybersecurity companies. The sources identified included items produced in Armenian, English and Russian.

Many of the items identified contained or drew upon sources of data widely regarded as robust and which are commonly included within academic literatures. These included official reports and statistics and academic research surveys. However, we are aware of potential issues of unreliability, bias, and a lack of robustness in some of the source types identified in this phase of the research. We sought to ensure validity in several ways. Drawing upon the national and international knowledge of the researchers and a research assistant, we excluded sources that we felt lacked national or international reputations for reliability. For example, in the case of media sources we drew only upon those sources we knew to be politically non-aligned and that had a multi-year track record of publication. Further, we tried to restrict the information that we extracted to that which could be verified through public records, such as reports of cases of cybercrime that had been prosecuted through the Armenian legal system, or, where they reported the views of those with local expertise, to those cases where that local expertise was publicly verifiable. Evaluation of the empirical information extracted from these sources suggested a high degree of internal correspondence, giving us confidence in the validity of the trends we report in the two subsequent sections. Where possible we tried to evidence the observations we made through multiple sources. Finally, the information obtained during the first phase of research was tested in the second phase, which consisted of a series of semi-structured expert interviews.

The experts for inclusion in phase two were selected through a purposive, non-probability search. This was problem- and expertise- oriented (von Soest, 2022: 3) and experts were selected on the basis of their publicly verifiable regional expertise in either cybercrime and

illicit internet use or conditions affecting young people in Armenia. 14 people with appropriate expertise were identified through this search who were contacted. Of these, eight agreed to be interviewed. Although the number of interviewees was relatively low, the pool of appropriate expertise from which these were drawn was also small and those who took part were reflective of the breadth of expertise identified in the wider pool. The high degree of correspondence in the information provided by the interviewees gives us confidence in the material collected in this phase. Details of the interviewees are given in the appendix.

The interviews were conducted between November 2021 and April 2022 using a variety of standard video calling software platforms. The interviews were recorded with consent. The interviews were semi-structured and qualitative in nature and, although the specific interview schedules were tailored to an extent to the specific expertise of the interviewee, they collectively covered: relevant biographical / professional / organisational information; policing, legislation and regulation of cybercrime and illicit internet use in Armenia; cybercrime in Armenia, trends, nature, extent and examples / cases; relevant socio-economic and political conditions affecting young people in Armenia; and the IT sector in Armenia.

The interviews all lasted between 33 minutes and one hour 17 minutes, with an average length of 44 minutes. All of the recorded interviews were listened to several times by both researchers. Transcripts were produced using speech to text software which were read several times and errors generated by the software corrected. This provided a thorough emersion in the interview material. The interviews were analysed through the application of thematic analysis.

Findings

Cyber-Criminogenic Conditions in Armenia This section considers the extent to which conditions identified within the cybercrime literature, with the potential to be cyber-criminogenic, are present in Armenia. . Internet penetration in Armenia is almost universal, a 2020 estimate suggested that 96 per cent of Armenians had access to the internet (Raja and Malumyan, 2020), whilst the internet is an important part of the lives of young people (Mkrtichyan, Vermishyan and Balasanyan, 2016), and social media use is high (Baghdasaryan, 2013; Data Reportal, 2020). This suggests the presence of developed socio-technological conditions in Armenia.

The legitimate economy in Armenia has experienced a number of negative trends in recent years, including economic downturn, stagnation, uncertainty, and high levels of

unemployment. The country was hit hard by the 2008 global financial crash (World Bank, 2015; Tiwari, Cancho, Meyer and Fuchss, 2018) and the subsequent decade was largely one of economic stagnation (Iskandaryan, 2018). The stronger economic growth witnessed towards the end of the last decade has since stalled due to the impacts of Covid-19 (World Bank, 2020). Young people appear to have been particularly badly impacted by these trends. Youth unemployment remains high in Armenia. A 2016 survey found that 55 per cent of young people over 23 who responded were unemployed (Mkrtichyan, Vermishyan and Balasanyan, 2016). Those affected by youth unemployment in Armenia include those with advanced education. The percentage of the labour force with advanced education who were unemployed in Armenia was 17.24 in 2020 (World Bank, 2022). For those young Armenians who are employed, it has been reported that their recent experiences of employment in Armenia have often been of low pay and job insecurity (Sargsyan and Cairns, 2019). Armenia, then, does appear to possess an impoverished legitimate economic context, which especially affects the lives of young people.

Some high cybercrime countries have been said to be characterised by widespread social tolerance and acceptance of illicit practices and actors, reflective of both a developed illicit economic context and a materialist social / cultural context. In Armenia, these are evident in the cultural and political accommodation of organised crime groups (Babayan, 2018; Mejlumyan, 2020), and the apparent acceptance of illicit practices as legitimate routes to prosperity (Mkrtichyan, Vermishyan and Balasanyan, 2016: 72; Medina and Schneider, 2018). It has been noted, for example, that "the role and significance of work–as the primary means to achieve prosperity–have considerably decreased in Armenian society. Professional work presents itself as an 'unprofitable' occupation" (Mkrtichyan, Vermishyan and Balasanyan, 2016: 43). These authors go on to observe that in Armenia "When financial success is considered to be the major aim for everyone, but there are no legal ways of achieving this aim within society, deviant behaviour increases and value disorientation comes into play" (72).

High levels of corruption have also been noted in Armenia (Feldman, and Alibašić, 2019; Kavkazkii, 2019; Iskandaryan, 2020). This appears to have infected sectors of the Armenian economy. Studies have recognised significant barriers facing young people accessing professional employment (Sargsyan and Cairns, 2019), associated with a widespread perception amongst young Armenians that corruption and nepotism are more important than

qualifications in finding a job (Mkrtichyan, Vermishyan and Balasanyan, 2016; Sargsyan and Cairns, 2019).

Nationalist political contexts that are tolerant of, or indifferent towards, external cyber economic or political victimisation, or within which it is actively promoted, have been drawn upon by cybercriminals in some high cybercrime countries, such as China and Nigeria (Kshetri, 2010; 2013b), to justify their activities by attaching discourses of patriotism to them. Such political motivations have been attached to recent online activities originating in Armenia including campaigns of economic cybercrime, hacking and fake news directed towards Azerbaijani and Turkish targets (HackRead, 2015a; 2015b; Kavkazkii, 2015; Martirosyan, 2017; News Armenia, 2017; ArmInfo, 2020; Mkrtchyan, 2020). It has been argued that these activities are reflective of the negative views of these groups in Armenian political and public discourse (Terzyan, 2018; Yerevan Press Club., 2019; Vetsko, 2020) suggesting some elements of strong nationalism within Armenia's political context.

Finally, a series of short comings in national anti-cybercrime measures have been recognised in Armenia including, the lack of a whole government approach to cyber security (Nerzetyan, 2018) and the relatively low number of convictions for cybercrime offences that have been secured (Israelyan, 2015). The Council of Europe's CyberEast Project (2019: 5), for example, noted the lack of a government Computer Emergency Response Team (CERT) "which poses great challenges for coordination and response". Inadequacies within the legal / regulatory and policing context in Armenia, was also a theme raised within our interviews. Several challenges were identified by our interviewees, in addition to those noted above. Giorgi Jokhadze (23 November 2021), from the CyberEast Project, who manages the Council of Europe's cybercrime projects with Eastern Partnership countries, of which Armenia is a member, identified problematic legacies of the Soviet era, limitations in Armenia's cybercrime policing and law enforcement capacity and issues of compliance with the Budapest Convention on Cybercrime. He noted, for example, that cybercrime policing is an unpopular area of police work due to low clearance rates which may hinder career progression. Jokhadze did, though note some improvements since the Velvet Revolution in 2018. Concerns about police capacity were also raised by Grigori Saghyan, secretary of the Internet Governance Council of Armenia who cited low police salaries compared to those available in the private sector diverting IT expertise away from cybercrime investigation (7 February 2022). A lack of policing capacity was confirmed in an interview with Vvahagn Harutyunyan (13 April 2022), ex-Head of the Anti-Cybercrime Unit of the Armenian Police,

who said, “I worked in cybercrime for 11 years. From 2009 to 2019. When I became Deputy Head of the Cybercrime division. at that time, the cybercrime unit was very poorly equipped. As in not enough computers. But it was also poorly staffed in terms of mind. They only really caught pornography”. He also noted the impacts of low police salaries on policing capacity in Armenia: “For now, we don’t have enough people (police) but you know the police income is also very low, lower than in other businesses, that’s why maybe people leave the police as they are in demand, they can even go abroad to the US or Europe and use their skills”. Nerses Kopalyan (15 December 2021), a Political Scientist from University of Nevada, Las Vegas, noted, with reference to the problematic legacies of the Soviet era, a reluctance of the state to engage with the private sector over cyber issues, a tendency for cybersecurity capacity in Armenia to be prioritised towards cyberwarfare rather than cybercrime investigation, reflecting Armenia’s regional geopolitical relations, and a lack of expert cybercrime prosecutors in Armenia.

In sum, this analysis suggests that a number of potentially cyber-criminogenic conditions are, to significant degrees, co-present within Armenia, which is suggestive of a national context that is potentially cyber criminogenic. The Armenian government, then, has pursued a policy of IT-focused development in recent years. This has taken place within the context of regional poverty, unemployment amongst young people, and the presence of the other conditions that may contribute to the regional growth of cybercrime.

Economic Cybercrime Trends in Armenia

Armenia does appear to be on an upward trajectory in terms of levels of economic cybercrime originating from and practiced there. It has seen recent spikes in fraud perpetrated over social media (Armenia Sputnik, April 2020; Council of Europe, 2019; 2020) and the theft of personal data for blackmail (Armenia Sputnik, July 2020). Rather than being new phenomena, resulting from the second Karabakh war and / or the Covid-19 pandemic, these are the continuation of trends that have been observable for some time. Whilst a lack of reliable data makes mapping cybercrime trends difficult, it has been widely recognised that Armenia has been experiencing growth in cybercrime for almost 10 years.

Wired magazine was able to claim in 2012 that “Armenia is not a leading haven for cybercriminals” (Zetter, 2012). In 2014 it was reported that, whilst cybercrime in Armenia was still not extensive, it was growing (JNews, 2014). This upward trend was confirmed in 2016 by Dmitry Beresnev, Head of Management and Control of Microsoft in CIS countries

(News Armenia, 2016). More recent reports, citing police sources, suggest 20-25 percent annual growth rates in cybercrime cases in Armenia between 2016 and 2018 (Armenpress, 2018), albeit from a low base, and by 2019, F-Secure, a Finnish cybersecurity company, identified Armenia as a new entrant in the world's top ten cybercrime source countries (F-Secure, 2019).

Empirically substantiating the broad trends noted above is a challenging endeavour, given the lack of robust data. There are relatively few publicly available discussions of specific cybercrime cases in Armenia. Those that are reported tend to contain only sparse details of the cases and those involved. The majority of reported cases involve individuals or pairs of conspirators involved in different scams including setting up fake social media accounts or advertisements with the intention of fraudulently obtaining loans, other forms of identity theft, blackmail and stealing money from bank ATMs (Investigative Committee, January, 2019; March 2019; April, 2019; January 2020; Novosti Armeniia., 2019). There is also discussion of Armenia's first conviction for a computer-related crime, the case of Georgy Avanesov a 27-year-old, who received a four-year prison sentence in 2012 for creating the Bredolab botnet (Zetter, 2012).

Other cases, though, involve the arrest of larger groups of between four and eight people engaged in more organised scams including thefts from money transfer systems, embezzlement by a group posing as loan mediators between banks and customers, theft using point of sale terminals obtained by registering fake hospitality companies, the Piconet Technology LLC case, a fake virus scam, and a scam targeting researchers by imitating the websites of two European scientific journals (ArmBanks, June, 2020; July 2020; Armenpress, March 2017; Butler, 2013; Papachristou, 2019). Some of these examples suggest degrees of sophistication and organisation reminiscent of cybercrime cases from other Eastern European and former Soviet states (Glenny 2011: 173-174). These cases, for example, involved extensive victimisation, a preliminary police investigation of the Piconet Technology case identified 60 US victims (Papachristou, 2019), the theft of significant sums of money, the case involving the point of sale terminals theft is reported to have netted 85 million Dram (worth roughly USD 172 000) from several Australian citizens (Armenpress, March 2017), and evidence of advanced technical expertise, the fake academic journal website case is reported to have duped hundreds of researchers into paying author fees and initially fooled Thomson Reuters, a metrics company who compile journal impact factors (Butler, 2013). Noting the upward trajectory in this economic cybercrime activity and instances of its success

and sophistication, suggests a more systematic review of Armenian cybercrime cases would extend our empirical understanding to a nation for which the academic literature presently offers no substantive discussions.

Despite the apparent upward trend noted above, there was universal consensus within our interviews that cybercrime in Armenia remains low and has not risen to match the levels observed in other nations in Eastern Europe and the former Soviet Union such as Russia, Romania and Ukraine (Glenny, 2011; Kshetri, 2013a; Lusthaus and Varese, 2017). Respondents were explicit in their view that economic cybercrime was not extensively practiced within Armenia.

> "We still view Armenia as a low crime country in terms of cyber, if you compare it to the data coming from Ukraine, which is of course quite telling, but also Belarus, for example, which is a sort of safer destination, or used to be" (Jokhadze, 23 November 2021).

> "I think we still have a long way to go to become like Romania [in terms of levels of cybercrime from there]" (Harutyunyan, 13 April 2022).

Whilst Giorgi Jokhadze noted there was a possible issue of under reporting of economic cybercrime in Armenia, stemming from the lack of a Government CERT, he did not feel this was a major or systemic omission and would not change the overall picture significantly.

The lack of any extensive cybercrime economy in Armenia was confirmed by other respondents. The economic cybercrime that was noted was generally characterised as minor.

> "These were mostly cases involving stealing via Facebook, card fraud and also from bank accounts. These were mainly Armenian bank accounts … It's mostly related to personal websites and social media sites. With small amounts of money. We had this case of a fraudster, where the fraudster got more than 33,000 Dram, this is 60 (US) dollars" (Harutyunyan, 13 April 2022).

> "Cybercrime coming out of Armenia is very, very minimal … From the domestic lens I am familiar with some cases of groups within Armenia who engage in cybercrime for economic reasons. They target, you know, external audiences, whether it is in the EU or United States, this is petty stuff" (Kopalyan, 15 December 2021).

> "We may say that there are special internet oriented crimes or internet oriented misbehaviour or something, but I cannot say there is something like phishing emails

> trying to get peoples' bank accounts or something like this, so there is no crime, I mean on a mass scale" (Ruben Muradyan, Chief Information Security Officer, in the Armenian IT sector, 20 December 2021).

It was noted by one respondent that the low levels of economic cybercrime observed in Armenia were reflective of its immediate regional context, where the Caucasus region is seen as somewhat behind wider cybercrime trends.

> "In our experience… the Caucasus region, I mean maybe with a bit of an exception with Georgia as Georgia is on the forefront when it comes to cybercrime, we don't see a lot of, you know, response to the global trends. So, for example, when we see that there is an advance somewhere that is a big problem, especially with virtual currencies, the units in Armenia do not report it as much. I mean they still report more traditional forms of fraud as being the main problem, and social engineering, especially by social networks, especially the Russian language ones, but they seem to be a bit lagging behind in terms of following the latest trends" (Jokhadze, 23 Novermber 2021).

There was a feeling, expressed by some respondents, that Armenia offers insufficient domestic opportunities for cybercrime, to sustain any extensive, internal cybercrime economy, and that domestic Armenian cybercriminals generally lacked the technical expertise or knowledge of potential target nations to launch actions directed externally, on any significant scale.

> "The vast majority of cybercrime is done at the domestic level, so cybercriminals in the US or in the UK or in France target people in UK, US or France. They usually operate domestically. Armenia's domestic market is so small that cybercriminals cannot operate, there is no market of crime in Armenia, so if you are a cybercriminal you have to operate externally, and this is a very complicated process… Because to engage in cybercrime you need to have a degree of healthy understanding of the country that you are targeting, their banking system, their credit card system, the behaviour of individuals you are trying to target, the type of fraud you are going to engage in. There are a lot of cultural components involved in that" (Kopalyan, 15 December 2021).

> "I don't think, like, the market for cybercrime in Armenia is near the level that it is in Ukraine… in Ukraine we've seen a lot of financially motivated scams, clickbait,

online, and in Armenia I haven't seen as much of that" (Zarine Kharazian, associate editor Atlantic Council, Digital Forensics Research Lab, 20 December 2021).

The individual cybercrime cases discussed in the Armenian media and reviewed above, do include some examples of sophisticated, externally directed scams, reaping victims from across Europe, the USA and Australia (Armenpress, March 2017; Butler, 2013; Papachristou, 2019). However, if the interpretations offered by our respondents are an accurate reflection of the nature of Armenian economic cybercrime, these would appear to be exceptions, rather than the norm.

There was some discussion within the interviews, of cybercrime activity, albeit still on a minor scale, being imported into Armenia from abroad, especially through diaspora networks from the United States.

> "As far as the cybercrime stuff that we are talking about, it's not indigenous, it's coming from the outside… So whatever behaviour we are seeing is being transported in, it's not something that is being organically developed from the inside… post Velvet [Revolution], like I said, it's basically, if I would say I have seen anything, or observed any patterns, its these small activities that are being transported from the outside, mainly from the United States into Armenia. So, if you are a criminal operative in the US and you engage in some wire fraud as they call it here, which is credit card or banking fraud, you know, simply doing it in Armenia and then changing your whatever, the IP… you would think you have some insulation post Velvet it's these sort of individualised, non-systemic activities that you are seeing being transported from outside of the country" (Kopalyan, 15 December 2021).

IT Development and Regional Poverty Interactions in Armenia

The previous section, whilst only able to offer a brief overview of recent trends in economic cybercrime in Armenia, recognised that, despite evidence of a rising trajectory since 2010, levels remain low and do not compare to those observed in other high cybercrime nations in Eastern Europe and the former Soviet Union. Armenia, then, differs from these nations. It has experienced the widely theorised and observed, apparently cyber-criminogenic, combination of IT development and ongoing regional poverty affecting young people. It is the co-presence of these factors within other nations that has produced a pool of appropriately skilled and motivated cybercrime labour. Despite this, Armenia has not developed into another post-Soviet high cybercrime nation.

This section, then, asks why extensive cybercrime growth has not occurred within Armenia, by exploring the specific interactions between IT development and regional poverty there. We recognise three characteristics of IT sector development in Armenia that mitigate against the growth of cybercrime. These are yet to be substantively discussed within the context of IT development there and offer potential policy lessons that might be transferable to other regional contexts.

First, Armenia's IT sector growth has been rapid, and has been sufficient to absorb the pools of appropriately skilled young people available in Armenia. In our interviews, Ruben Muradyan, who works at a senior level within the growing IT sector, described the effect of this growth as akin to that of a "vacuum cleaner".

> "For the last two decades the IT sector is blooming, and it acts like a vacuum cleaner that is sucking up all of the engineers from nearby areas of specialisation. If a person has gone through higher mathematics during his university studies, he is ready to become a software developer, or a system administrator, or a network engineer, or you name it" (20 December 2021).

The receipt of IT investments and relocations from overseas companies, especially from the US through diaspora connections, and more recently Russia, following the imposition of international sanctions, were identified in interviews as important in fuelling the growth of Armenia's IT sector, (see also Avestisyan, 2022).

> "The IT sector in Armenia went from basically being seven percent of the economy to 14 percent, and now it's at 18 percent. About three, four very large companies out of the US such as ServiceTitan, for example, you know, they're friends from high school, they're moving a chunk of their one-billion-dollar company into Armenia" (Kopalyan, 15 December 2021).

> "You know what, because of the sanctions against Russia, lots of people from Russia, Armenians from Russia but also just Russians, they come to Armenia, open up their own business, 90 percent of them are programmers, let's say or work in this sphere. I'd say that IT takes the first place and is our expertise. Pashinyan did say it right that there is a lack of skilled people because the potential of this area is huge" (Harutyunyan, 13 April 2022).

We do not see in Armenia, then, the situation observed elsewhere, of large numbers of young people with IT skills, unable to find legitimate employment opportunities commensurate with

their skills and aspirations, who turn to cybercrime. Indeed, in Armenia, there is evidence of an under-supply of appropriately skilled IT labour (EU4Digital, 2019), something confirmed in our interviews.

> "Right now, you do have severe shortages in the workforce. Most IT companies that operate in Armenia actually have a work[force] shortage, they have a shortage of IT experts… So, it's not as if you have a large number of qualified IT experts who can't find jobs. It's actually the very reverse. There is a very very strong need for programmers, for engineers in the IT sector The market has a huge demand, but Armenia's IT sector, at least the workforce, isn't able to supply that demand at this point… It's not at a point where you have unemployed experts that might engage in illicit behaviour, it's actually the complete opposite, you don't have enough experts to meet the demands of the market" (Kopalyan, 15 December 2021).

Training young people with IT skills in Armenia, and their gaining employment has not been a straightforward process, however. Although, in Armenia the Soviet technological legacy "is still alive today in how the country embraces education and hard sciences" (Shepard, 2020: no page), this has not resulted in high quality education and training that is responsive to the needs of business. Armenia, for example, performs poorly in maths and science education compared to other former Soviet states (Caro and He, 2018). Further, the World Bank reported that only 45 per cent of Armenian IT graduates were considered sufficiently skilled to enter the workforce (World Bank, 2014). The connections between scientific talent and business, in Armenia, therefore, do not appear to be seamless, something articulated by the team behind the tech start-up Krisp, for example (Mkrtumyan, 2019b) and may have only exacerbated the shortages of skilled IT labour noted above. Thus, our respondents were all able to confirm the recent rapid growth of the Armenian IT sector in absolute terms and its capacity to absorb the pools of skilled young people available.

Second, salaries within Armenia's growing IT sector are high, within the context of Armenia's economy (Avetisyan, 2022), and are sufficient to deter migration towards alternative illegal economic opportunities. The experiences of young people working within Armenia's growing IT sector differ significantly to those encountered in other sectors (Parsyan, 2021). The issues of low pay and job insecurity that have been identified as affecting young people in Armenia (Sargsyan and Cairns, 2019) do not apply to the IT sector. This was an issue unanimously identified across the interviews that we conducted.

> "maybe you're working for an American company that is based in Armenia, that has a, you know, sort of, presence in Armenia and generally, yeah, you are paid a better salary than you would if you did not work in the tech sector" (Kharazian, 20 December 2021).

> "When we talk about corruption and poverty, that is not applicable to the IT sector because, actually those in the IT sector are the upper middle class in Armenia. So, if the average income in Armenia is about 400 dollars a month, those in the IT sector are making 17, 18 [hundred], 2000 dollars a month … because the average IT worker makes 15, 16 hundred dollars a month which is extremely well paid in Armenia, there's really no relationship between poverty and this sector. It's actually the reverse. This is why I don't see someone who's, you know, making the equivalent of what would be 100, 150 thousand dollars US or 100 thousand pounds [1]20 thousand pounds in the UK, engaging in cybercrime when they have an extremely well-paying job and a very comfortable lifestyle" (Kopalyan, 15 December 2021).

> "So, when you say that someone [with IT skills or working in the Armenian IT sector] would, or should, or can, or perhaps could be involved in illicit internet use or cybercrime, or something, those people do not have reasons to do it. They are earning ten times more than other salaries if they are on a senior level. So just imagine the social gap between all the regular average people and people working in ICT" (Murdyan, 20 December 2021).

Third, as Nerses Kopalyan indicated above, and other respondents confirmed, the IT sector is largely free of the corruption and nepotism characteristic of other sectors in the Armenian economy (Mkrtichyan, Vermishyan and Balasanyan, 2016; Sargsyan and Cairns, 2019). In terms of young people's experiences, this means that this sector is more oriented towards the qualifications and skills of employees than their social connections and young people with appropriate qualifications and skills do not face the barriers to entry that they might encounter in other sectors. Our interviewees attributed the lack of corruption in this sector to the high salaries of the IT sector, the high degrees of involvement by overseas companies and the lack of connections to government.

> "So, in the IT sector, both poverty isn't an issue and corruption is simply not applicable to that industry because it really has no relationship with the government or

with government contracts or processes that are conducive to corruption" (Kopalyan, 15 December 2021).

"This is [working in the Armenian IT sector] the area where the most possible meritocracy within a transitional society like ours is implemented. I mean it will not be implemented, it is already implemented" (Muradyan, 20 December 2021).

"In Armenia, most IT companies work as part of other companies based abroad. I have a friend programmer for example who works for an educational company based in Malaysia. Another friend of mine is writing an IT project for a company based in Singapore. Others design websites for European companies" (Harutyunyan, 13 April 2022).

Kopalyan also indicated that structurally the Armenian IT sector is geared towards start-up companies (see also, Avetisyan, 2022), and suggested that career frustration within the sector could be more easily resolved by leaving a job and creating a start-up, rather than by engaging in cybercrime. He also cited the post-revolutionary values, high ethical standards and professional identities of young people involved in the Armenian IT as further mitigation against their involvement in cybercrime.

"I would see that the culture and the ethics within the IT sector, are very very high. The etiquette is very very high because those in the IT sector view themselves as being highly professional. They do view themselves as being the very opposite of what the previous system was. So, within the bubble that is the IT sector, in that culture actually these kinds of behaviour [cybercrime] is looked down upon. It's frowned upon and they are the ones who are displaying some anger and frustration at the, sort of, diaspora elements trying to trickle down cybercriminal behaviour because, the point is, we have such a positive reputation internationally that we don't want anything harming this reputation. So, in that context I would argue that you would see very very serious pushback from the industry if any of this illicit behaviour grows or becomes an issue" (Kopalyan, 15 December 2021).

Whilst this might suggest there are structural and cultural components that have also distanced the Armenian IT sector from illegality, these are not issues that arose in other interviews, however, so might be considered, for the moment, areas that would merit further investigation.

In sum, then, this discussion indicates that, despite being spatially co-present, there is very little, or no, interaction between the IT sector in Armenia, and those engaged within it, and the high levels of regional poverty and corruption observed within the nation. The ready availability of jobs, the high salaries paid, and the lack of barriers to entry for those with appropriate qualifications and skills, mean that young people involved in this sector are able to avoid the challenges that affect their peers in other sectors. The exceptional nature of the IT sector within the context of the wider Armenian economy was captured by two, possibly throwaway, comments from our interviews. It was described as like a "vacuum cleaner" (Muradyan) and a "bubble" (Kopalyan).

The final section of this paper now goes on to draw out some wider implications of this case.

Conclusions

Earlier we outlined three scenarios that might potentially result from IT development occurring in the context of regional poverty. Of these, Armenia seems most likely to have experienced the second: IT development accompanied by sufficient IT jobs growth, sees no resultant rise in cybercrime. Although we noted some discussions of rises in economic cybercrime in Armenia, we found no evidence to connect this to IT development there, and Armenia continues to be perceived as a low cybercrime nation. Further, we can dismiss the first scenario: IT development not accompanied by sufficient IT jobs growth, sees a resultant rise in cybercrime. Our interviews clearly indicate that IT jobs growth in Armenia has at least matched the supply of skilled labour in recent years. Indeed, it is likely to have exceeded this supply during this time.

We can confidently conclude, therefore, that IT development in Armenia has not produced a resultant rise in cybercrime. Our first policy lesson from this case should be that IT development can, under certain circumstances, occur within the context of regional poverty, and other potentially cyber-criminogenic conditions, without a resultant rise in cybercrime. The characteristics of the Armenian case, outlined in the previous section, might inform the principles of any future policy model. Namely, IT development in the context of regional poverty and other potentially cyber-criminogenic conditions should: be able to absorb the supply of IT-specialist labour; generate salaries that are sufficient to deter illegality; and ensure that entry is based only on qualifications and skills.

However, we should remain wary of assuming the universal transferability of the Armenian model. Defining specific policy objectives, the ways in which the principles above are to be

achieved, that do not generate unintended cyber-criminogenic outcomes, present significant challenges. Our interviews identified particularities of the Armenian case that mitigated against cybercrime illegality. These were, the roles of overseas investment and involvement, especially through diaspora connections to the United States, as significant drivers and shapers of Armenia's IT development and, perhaps, the post-revolutionary cultural orientations of young people involved in IT. The challenge for policy transfer from this case is likely to involve designing policy objectives that replicate the effects of these particularities across very different demographic, economic and social contexts.

At this point we are unable to say anything definitive about the third scenario outlined earlier: IT development accompanied by sufficient jobs growth sees a resultant drop in cybercrime, or slowing of growth. The potential of IT development being deployed as a form of explicit anti-cybercrime policy, then, remains an open question and an avenue of further research.

This paper has also advanced a series of theoretical contributions. It acknowledges the range and diversity of potentially cyber-criminogenic factors identified across salient literatures (Hall et al., 2021) We also recognise the particular importance attached to developed socio-technological and impoverished legitimate economic conditions, in explaining the presence of extensive cybercrime economies within certain regions. However, the analysis presented here suggests such combinations of conditions will also be present in regions without extensive cybercrime economies. We cannot, therefore, interpret the geographies of cybercrime solely through the spatial co-presence of certain conditions, or through statistical correlation alone. Our analysis emphasises the importance of also demonstrating causality by exploring specific interactions between potentially cyber-criminogenic conditions within regions. This points to the value of more ethnographic approaches. We would recommend that future analysis also considers ranging beyond the familiar terrains of Eastern Europe and West Africa that have monopolised the literatures of cybercrime to date. It should consider pursuing new, or little recognised, cybercrime threats, or cases like Armenia that might challenge the prescriptions of universal models of cybercrime.

Finally, this analysis suggests several Armenia specific avenues of further research. First, a systematic analysis of Armenian cybercrime cases would add further empirical validity to the arguments within this paper and would reveal much about the nature, levels and types of economic cybercrime practiced within Armenia, and its organisation, sophistication and patterns of victimisation. Second, an economic analysis of the IT sector in Armenia covering its structure, the roles of overseas investment and involvement, especially through Armenia's

diaspora connections, and profiles of those involved, would help us understand more, how it has evaded the problems of low growth, low salaries and corruption that have blighted other sectors of the Armenian economy. Third, the equitable distribution of the costs and benefits of Armenia's IT development, across other sectors of the economy and society, also remains an open question, worthy of further investigation. Fourth, future research should speak more directly to young peoples' experiences of living through the transitions discussed here. Surveys that engage directly with young Armenian's employment experiences, self-identities and cultural orientations would add considerable nuance to our understandings of the multiple ways in which they are negotiating a potentially cyber-criminogenic environment. Finally, the Armenia case might be used to ask broader, regional questions about cybercrime threats and the factors that underpin them. There is a tendency, in both the popular imagination and in some cybercrime literature, to see the former Soviet Union as an undifferentiated cyber-threat scape. The Armenia case suggests there is greater nuance to this regional context than has generally been acknowledged. Situated analysis across this region would help excavate differences in the specific geographies of the post-Soviet cyber-threat landscape.

Acknowledgements

This research has been supported by a British Academy small research grant (award number: SRG1920\100892). We would like to thank Eva Rosenthal for her invaluable research assistance on this project.

References

Adeniran A. (2011) 'Cafe culture and heresy in Yahooboyism in Nigeria', in Jaishankar K, (ed) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*, Boca Raton, FL: CRC Press, 3–12

ArmBanks., (June 2020). Head of credit organization and his subordinates accused of fraud and embezzlement. *ArmBanks*. [Accessed 29/10/2020]. Available at: https://www.armbanks.am/en/2020/06/17/129274/

ArmBanks., (July 2020). Cybercriminals steal 18 million drams from Adjarabet, EasyPay and TelCell terminals in Armenia. *ArmBanks*. [Accessed 29/10/2020]. Available at: https://www.armbanks.am/en/2020/07/07/129570/

Armenia Sputnik., (December 2017). Internet-grabli: pochemy armiane nikak ne mogut ot nikh izbavit'sia? *Armenia Spunik*. [Accessed 25/11/2020]. Available at:

https://ru.armeniasputnik.am/society/20171224/9933144/internet-grabli-pochemu-armyane-nikak-ne-mogut-ot-nih-izbavitsya.html

Armenia Sputnik., (August 2018). Khakery natselilis'na Armeniiu: delat' onlain pokupki stalo nebezopasno? *Armenia Sputnik*. [Accessed 25/11/2020]. Available at:

https://ru.armeniasputnik.am/society/20180808/13744381/hakery-nacelilis-na-armeniyu-delat-onlajn-pokupki-stalo-nebezopasno.html

Armenia Sputnik., (April 2020). Moshenniki aktivny ne tol'ko v Armenii: chislo kiberprestuplenij v Rossii rezko vyroslo. *Armenia Sputnik*. [Accessed 30/10/2020]. Available at: https://ru.armeniasputnik.am/russia/20200415/22737538/Moshenniki-aktivny-ne-tolko-v-Armenii-chislo-kiberprestupleniy-v-Rossii-rezko-vyroslo.html

Armenia Sputnik., (June 2020). Na grani kibervoiny, ili Chem grozit armiano-azerbaidzhanskii "koronovarusnyi sliv". *Armenia Sputnik.* [Accessed 9/11/2020]. Available at: https://ru.armeniasputnik.am/politics/20200626/23531459/Armeniya-i-Azerbaydzhan-na-grani-kibervoyny-ili-Chem-grozit-koronavirusnyy-sliv.html

Armenia Sputnik., (July 2020). Rost kiberprestuplenii v Armenii: kak ne stat' zhertvoi internet-lovkachei? Armenia Sputnik. [Accessed 27/10/2020]. Available at: https://ru.armeniasputnik.am/society/20200710/23678321/Rost-kiberprestupleniy-v-Armenii-kak-doverchivym-grazhdanam-ne-ugodit-v-seti-moshennikov.html

Armenpress., (August 2016). Kiberprestupnost' ugrozhaet kazhdomy tret'emu zhiteliiu Armenii. *Armenpress.* [Accessed 29/10/2020]. Available at: https://armenpress.am/rus/news/858296

Armenpress., (March 2017). Armenia's national security service uncovers transnational crime syndicate. *Armenpress S*. [Accessed 29/10/2020]. Available at: https://armenpress.am/eng/news/883187/armenia%E2%80%99s-national-security-service-uncovers-transnational-crime-syndicate.html

Armenpress., (June 2018). Armenia police warn of growing cybercrime rate. *Armenpress*. [Accessed 29/10/2020]. Available at: https://armenpress.am/eng/news/937066/

ArmInfo., (15 July 2020). Armenian hackers hacked site of Azerbaijani Anti-Armenia Team. *ArmInfo*. [Accessed 9/11/2020]. Available at: https://arminfo.info/full_news.php?id=53642&lang=3

Armstrong A (2011) *'Sakawa' Rumours: Occult Internet Fraud and Ghanaian Identity*, UCL anthropology working papers series, working paper no. 08/2011, University College London, London

Avetisyan, A. (2022) 'Big talk, fast growth but still early stage: Armenia's tech industry', *EVN Report*, 28 April, Big Talk, Fast Growth But Still Early Stage: Armenia's Tech Industry - EVN Report [Accessed 29th April 2022]

Babayan, E. (2018). "Vor v zakone byl chut' li ne v kazhdom dvore." Kriminal'nye avtoritety zhili v Armenii spokoino. No u novoi vlasti svoi pravila. *Lenta.ru*. [Accessed 11/02/2021]. Available at: https://lenta.ru/articles/2018/07/16/nikol_i_vory/

Baghdasaryan, L. (2013). Facebook in Armenia. Users and Using. *OSCE*. [Accessed 05/01/2021]. Available at: OSCE – Facebook in Armenia

Burrell J. (2008) 'Problematic empowerment: west African internet scams as strategic misrepresentation', *Information Technology and International Development*, 4, 4: 15–30

Butler, Declan., (March 2013). Sham journals scam authors. *Nature*. [Accessed 25/11/2020]. Available at: https://www.nature.com/news/sham-journals-scam-authors-1.12681

Caro, D., and He, J. (2018). Equity in Education in Armenia: Evidence from TIMSS 2003-2015. Report. *Open Society Foundations – Armenia*. Available at: http://www.osf.am/wp-content/uploads/2018/05/Report-1-Equity-analysis-TIMSS-15-updated-25april.pdf [Accessed 12/09/21]

Council of Europe., (January 2019). Perception of threats and challenges of cybercrime in the Eastern Partnership, 2018 [report]. *Council of Europe*. [Accessed 25/11/2020]. Available to download from: https://www.coe.int/en/web/cybercrime/cybereast

Council of Europe., (2020). CyberEast Interview: On the Work of the New Department for Investigation of Cybercrimes and High Technology Crimes (DICHTC) within the Investigative Committee of Armenia. *Council of Europe.* [Accessed 28/10/2020]. Available at: https://www.coe.int/en/web/cybercrime/-/cybereast-interview-on-the-work-of-the-new-department-for-investigation-of-cybercrimes-and-high-technology-crimes-dichtc-within-the-investigative-comm

Digital Report., (April 2018). Armenia: State of Affairs report. Country Snapshot. *Digital Report*. [Accessed 25/11/2020]. Available at: https://digital.report/armenia-state-of-affairs-report/

Data Reportal., (2020). Digital 2020: Armenia. *Data Reportal*. [Accessed 05/01/2021]. Available at: https://datareportal.com/reports/digital-2020-armenia

Ekho K., (February 2019). Bolee treti pol'zovatelei v Armenii v 2018 podverglis' internet-atakam. *Ekho Kavkaza*. [Accessed 9/11/2020]. Available at: https://www.ekhokavkaza.com/a/29757290.html

EU4Digital., (May 2019). Training young people for a digital future in Armenia's regions. *EU4Digital*. [Accessed 05/01/2021]. Available at: https://eufordigital.eu/training-young-people-for-a-digital-future-in-armenias-regions/

Feldman, D. L., and Alibašić, H. (2019). The Remarkable 2018 "Velvet Revolution": Armenia's Experiment Against Government Corruption. *Public Integrity*, **21**(4), 420-432, Available at: http://dx.doi.org/10.1080/10999922.2019.1581042

F-Secure., (2019). Attack Landscape H2 2019/ Attack Landscape H1 2019. *F-Secure*. [Accessed 25/11/2020]. Available to download at: https://blog.f-secure.com/attack-landscape-h2-2019-an-unprecedented-year-cyber-attacks/ and https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

Glenny M, (2008) *McMafia: Crime Without Frontiers*, Bodley Head, London

Glenny M, (2011) *Dark Market: Cyberthieves, Cybercops and You*, Bodley Head, London

HackRead., (2015a). Armenian Group Hacks Azerbaijan Central Bank, Leaks A Trove of Data. *HackRead*. [Accessed 9 Novemver 2020]. Available at: https://www.hackread.com/armenian-group-hacks-azerbaijan-central-bank/

HackRead., (2015b). Armenian Hackers Leak Sensitive Data from Azerbaijan Ministry Servers. *HackRead*. [Accessed 9/11/2020]. Available at: https://www.hackread.com/armenians-hackers-hack-azerbaijani-ministry-servers/

Hall, T., Sanders, B., Bah, M., King, O. and Wigley, E. (2021) 'Economic geographies of the illegal: the multiscalar production of cybercrime', *Trends in Organized Crime*, 24, 2: 282-307

Ibrahim S, (2016a) 'Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals', *International Journal of Law, Crime and Justice*, 47: 44-57

Investigative Committee., (January 2019). Attempt to Swindle Money in Large Amount Editing Personal Data of Bank Client; Charge Pressed [online]. *Investigative Committee of*

the Republic of Armenia. [Accessed 27/10/2020]. Available at: http://www.investigative.am/en/news/view/banki-ashxatakic-hapshtakutyan-porc.html

Investigative Committee., (March 2019). Preliminary Investigation of Criminal Case Separated from Case on Swindling from ATMs Completed; Charge Pressed against 20-Year-Old RF Citizen [online]. *Investigative Committee of the Republic of Armenia*. [Accessed 27/10/2020). Available at: http://investigative.am/en/news/view/konvers-bank-hapshtakutyun-bankomatner.html

Investigative Committee., (April 2019). Within Criminal Case on Swindling Committed from Payment Terminals of "Converse Bank" Charge Pressed against One More RF Citizen [online]. *Investigative Committee of the Republic of Armenia*. [Accessed 27/10/2020). Available at: http://investigative.am/en/news/view/konvers-ban-bankomatner-rd-qaxaqaci-mexdranq.html

Investigative Committee., (January 2020). Charge Pressed Against 27-Year-Old Woman for Theft by Means of Computer; Case Sent to Court [online]. *Investigative Committee of the Republic of Armenia*. [Accessed 27/10/2020]. Available at: http://investigative.am/en/news/view/27-amya-axjik-hapshtakutyun-hamacancov.html

Iskandaryan, A. (2018). The Velvet Revolution in Armenia: How to Lose Power in Two Weeks. *Demokratizatsiya: The Journal of Post-Soviet Democratization*, 26(4), 465-482. [Accessed 18/01/2021]. Available at: https://search-proquest-com.libproxy.ucl.ac.uk/docview/2129462379?pq-origsite=primo

Iskandaryan, A. (2020). Armenia. In: L. Broers and G.M. Yemelianova, eds. *Routledge Handbook of the Caucasus* [online]. London: Routledge

Israelyan, I., (October 2015). Grigorii Saghyan, vitse-prezident ISOS-Armeniia: "Svobodnyi internet – zalog razvitiia". *Digital Report*. [Accessed 30/10/2020]. Available at: https://digital.report/isoc-armenia/

JNews., (2014). Tracing Cybercrime. JNews. [Accessed 29/10/2020]. Available at: http://www.jnews.am/en/cybercrime-in-Armenia

Kassarjian, R. (2017) 'Tech in Armenia: dawn of a new era?', *EVN Report*, 18 April, Tech in Armenia: Dawn of a New Era? - EVN Report [Accessed 27 April 2022]

Kavkazkii U., (7 September 2015). Saity trekh posol'stv Azerbaidzhana podverglis' khakerskim atakam. *Kavkazkii Uzel.* [Accessed 9/11/2020]. Available at: https://www.kavkaz-uzel.eu/articles/268450/

Kavkazkii U. (2019). Kakie tseli reshaet i k chemu privedet ob'iavlennaia bor'ba s organizovannoi prestupnost'iu? Armeniia kopiruet opyt Gruzii. *Kavkazkii Uzel*. [Accessed 02/02/2021]. Available at: https://www.kavkaz-uzel.eu/blogs/83781/posts/40591

Kigerl, A. (2012) 'Routine activity theory and the determinants of high cybercrime countries', *Social Science Computer Review*, 30, 4: 470-486

Kigerl, A. (2016a) 'Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates', *International Journal of Cyber Criminology*, 10, 2: 147-169

Kigerl, A. (2016b) 'Email spam origins: does the CAN SPAM act shift spam beyond United States jurisdiction?', *Trends in Organized Crime*, 21, 1: 62-78

Kshetri, N (2009) 'Positive externality, increasing returns and the rise in cybercrimes', *Communications of the ACM*, 52(12): 141-144

Kshetri N (2010) 'Diffusion and effects of cyber-crime in developing economies', *Third World Quarterly*, 31 (7): 1057–1079

Kshetri N (2013a) 'Cybercrimes in the former Soviet Union and central and Eastern Europe: current status and key drivers', *Crime, Law and Social Change*, 60 (1): 39–65

Kshetri, N. (2013b) 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations', *Electronic Commerce Research*, 13 (1): 41-69

Lazarus S. (2018) 'Birds of a feather flock together: the Nigerian cyber fraudsters (yahoo boys) and hip hop artists', *Criminology Crime Justice Law and Society*, 19, 2:63–81

Leukfeldt, E. R. (2014) 'Cybercrime and social ties: Phishing in Amsterdam', *Trends in Organized Crime*, 17, 4: 231-249

Leukfeldt. E. R., Kleemans, E. R. and Stol, W. P. (2017) 'Origin, growth and criminal capabilities of cybercriminal networks: an international empirical analysis', *Crime, Law and Social Change*, 67, 1: 39-53

LloydsBankTrade. (2022) *Armenia: Economic and Political Overview*, The economic context of Armenia - Economic and Political Overview - International Trade Portal International Trade Portal (lloydsbanktrade.com) [Accessed 27 April 2022]

Lusthaus J, and Varese F, (2017) 'Offline and local: the hidden face of cybercrime', *Policing: A Journal of Policy and Practice* doi.org/10.1093/police/pax042

Lusthaus, J., Bruce, M. and Phair, N. (2020) 'Mapping the geography of cybercrime: a review of indices of digital offending by country', *IEEE European Symposium on Security and Privacy Workshops (Euro S&PW)*: 448-453

Martirosyan, S., (May 2017). Istoriia armianskogo xakerstva, chast' V, 2013- nashi dni: byt' khakerom – modno. *Digital Report*. [Accessed 29/11/2020]. Available at: https://digital.report/istoriya-armyanskogo-hakerstva-chast-v-2013-nashi-dni-byit-hakerom-modno/

Medina, L. and Schneider, F. (2018). IMF Working Paper 18/17. Shadow Economies Around the World: What Did We Learn Over the Last 20 Years. *International Monetary Fund*. [Accessed 20/01/2021]. Available at: https://www.imf.org/en/Publications/WP/Issues/2018/01/25/Shadow-Economies-Around-the-World-What-Did-We-Learn-Over-the-Last-20-Years-45583

Mejlumyan, Ani., (23 January 2020). Armenia takes on "thieves in law". *Eurasianet*. [Accessed 20/01/2021]. Available at: https://eurasianet.org/armenia-takes-on-thieves-in-law

Mejlumyan, Ani., (February 2020). Armenia debates cracking down on "fake news" and hate speech. *Euriasianet.* [Accessed 2 Novemeber 2020]. Available at: https://eurasianet.org/armenia-debates-cracking-down-on-fake-news-and-hate-speech

Mezzour, G. L., Carley, R. and Carley, K. M. (2014) *Global Mapping of Cyber Attacks*, Pittsburgh PA.: Carnegie Mellon University

Mkrtchyan, Gayane., (22 October 2020). Taking the Karabakh Conflict Online. *Institute for War and Peace Reporting*. [Accessed 7/11/2020]. Available at: https://iwpr.net/global-voices/taking-karabakh-conflict-online

Mkrtichyan, Artur., Vermishyan, Harutyun., and Balasanyan, Sona., (2016). *Independence Generation Youth Study 2016 – Armenia*. Yerevan: Friedich-Ebert-Stiftung. Available at: https://hkdepo.am/en/resources/independence-generation-youth-study-2016---armenia

Mkrtumuan, T. (2019a) 'Placing Armenia on the global tech map', EVN Report, 2 July, Placing Armenia on the Global Tech Map - EVN Report [Accessed 27 April 2022]

Mkrtumyan, T., (2019b). Armenian Startups in Deep Tech: How Krisp is Breaking New Ground. *EVN Report*. 3 October [Accessed 05/01/2021]. Available at:

https://www.evnreport.com/economy/armenian-startups-in-deep-tech-how-krisp-is-breaking-new-ground

Nerzetyan, A., (March 2018). Information Security or Cybersecurity? Armenia at a Juncture Again. EVN Report. [Accessed 29/10/2020]. Available at: https://www.evnreport.com/economy/information-security-or-cybersecurity-armenia-at-a-juncture-again

News Armenia., (November 2016). Kiberprestupnost' v Armenii nakhoditsia esche v faze razvitiia – ekspert. *News Armenia*. [Accessed 30/10/2020] Available at: https://newsarmenia.am/news/armenia/kiberprestupnost-v-armenii-nakhoditsya-eshche-v-faze-razvitiya-ekspert/

News Armenia., (6 April 2017). "Armianskaya kiber-armiia Monte Melkonian" vzlomala krupneishii Azerbaidzhanskii forum. *News Armenia*. [Accessed 9/11/2020] Available at: https://newsarmenia.am/news/armenia/armyanskaya-kiber-armiya-monte-melkonyan-vzlomala-krupneyshiy-azerbaydzhanskiy-forum/

Novosti Armeniia., (October 2019). Moshennik v Armenii vymogal u zhenschiny den'gi pod ugrozoi publikatsii prochascshei informatsii. Novosti Armeniia. [Accessed 20/10/2020]. Available at: https://newsarmenia.am/news/incidents/moshennik-v-armenii-vymogal-u-zhenshchiny-dengi-pod-ugrozoy-publikatsii-porochashchey-informatsii/

Okeshola F B and Adeta A K. (2013) 'The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria', *American International Journal of Contemporary Research*, 3, 9: 98–114

Olayemi O J (2014) 'A socio-technological analysis of cybercrime and cyber security in Nigeria', *International Journal of Sociology and Anthropology*, 6, 3: 116–125

Papachristou, Lucy., (May 2019). Hetq: Police Raid Cybercriminals in Wake of Investigation. *OCCPR.* [Accessed 28/10/2020]. Available at: https://www.occrp.org/en/daily/9680-hetq-police-raid-cybercriminals-in-wake-of-investigation

Parsyan, S. (2021) 'The IT sector in Armenia is forming a middle class', *EVN Report*, 13 July, The IT Sector in Armenia Is Forming a Middle Class - EVN Report [Accessed 27 April 2022]

Raja, S., and Malumyan, G., (2020). Internet use in Armenia: How do individuals and businesses use the internet to access opportunities? *World Bank Blogs*. [Accessed

05/01/2021]. Available at: https://blogs.worldbank.org/europeandcentralasia/internet-use-armenia-how-do-individuals-and-businesses-use-internet-access

Sargsyan, Marine., and Cairns, David., (2019). Home or Away? Pathways to Employment for the Highly Qualified in Armenia After the Velvet Revolution. *Young*. 28, 3: 259-274

Shepard, Wade., (31 January 2020). Welcome To The World's Next Tech Hub: Armenia. *Forbes*. [Accessed 05/02/2021]. Available at: https://www.forbes.com/sites/wadeshepard/2020/01/31/welcome-to-the-worlds-next-tech-hub-armenia/

Tade, O. (2013) 'A spiritual dimension to cybercrime in Nigeria: the "yahoo plus" phenomenon', *Human Affairs*, 23, 4: 689-705

Tade O, and Ibrahim A. (2011) 'Social organization of internet fraud among university undergraduates in Nigeria', *International Journal of Cyber Criminology*, 5, 2: 860–875

Terzyan, A., (2018). Identity conflicts? The sense of victimhood and the enemy images of Turkey and Azerbaijan in the foreign policy discourse of Armenia. *Slovak Journal of Political Sciences*, 18, 2: 155-179

Tiwari, S., Cancho, C., Meyer, M., and Fuchss, A., (2018). South Caucasus in Motion. Economic and Social Mobility in Armenia, Azerbaijan and Georgia. *The World Bank Group*. [Accessed 17/01/2021]. Available at: https://doi.org/10.1596/1813-9450-8329

Tosunyan, S. (2021) 'Armenia: the Silicon Valley of the Soviet Union', *EVN Report*, 29 August, Armenia: The Silicon Valley of the Soviet Union - EVN Report [Accessed 27 April 2022]

Vetsko, Nika., (8 October 2020). Armenian, Azeri Youth Speak Out For Peace. *Institute for War and Peace Reporting*. [Accessed 13/01/2021]. Available at: https://iwpr.net/global-voices/armenian-azeri-youth-speak-out-peace

von Soest, C. (2022) 'Why do we speak to experts? Reviving the strength of the expert interview method', *Perspectives on Politics*, 1-11 doi:10.1017/S1537592722001116

Warner, J. (2011) 'Understanding cyber-crime in Ghana: a view from below', *International Journal of Cyber Criminology*, 5, 1: 736– 749

Whitty, M. T. (2018) '419 – it's just a game: pathways to cyber-fraud criminality emanating from West Africa', *International Journal of Cyber Criminology*, 12, 1: 97-114

World Bank., (2014). *IT Skills Assessment in Armenia (English)*. [Report]. Washington, DC: World Bank Group. [Accessed 04/01/2021] Available at: http://documents.worldbank.org/curated/en/105521468236363324/IT-skills-assessment-in-Armenia

World Bank., (2015). *Social Snapshot and Poverty in Armenia - Main Outcomes of 2014 Household Integrated Living Conditions Survey. Press Release*. [Online] [Accessed 03/02/2021]. Available at: https://www.worldbank.org/en/news/press-release/2015/11/23/social-snapshot-and-poverty-in-armenia-main-outcomes-of-2014-household-integrated-living-conditions-survey

World Bank., (2020). *The World Bank in Armenia. Recent Economic Developments*. The World Bank. [Accessed 17/01/2021]. Available at: https://www.worldbank.org/en/country/armenia/overview#3

World Bank (2022) Unemployment with Advanced Education, https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS [Accessed 25/4/22]

Yerevan Press Club., (2019). Armenia-Azerbaijan: Searching for New Models of Dialogue. *Yerevan Press Club*. [Accessed 12/01/2021]. Available at: https://ypc.am/studies/armenia-azerbaijan-searching-for-new-models-of-dialogue/

Zetter, Kim., (23 May 2012). Bredolab Bot Herder Gets 4 Years for 30 Million Infections. *Wired*. [Accessed 28/10/2020]. Available at: https://www.wired.com/2012/05/bredolab-botmaster-sentenced/

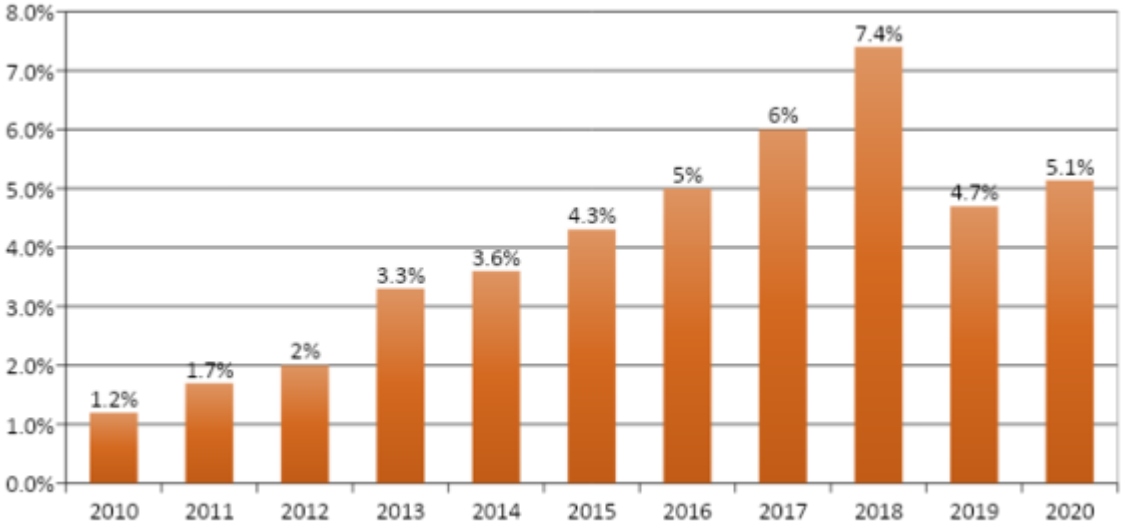

Figure 1: The share of the IT sector in the GDP of the Republic of Armenia in 2010-2020 (Adopted from Parsyan 2021, with permission of EVN Report).

Anthropologist, University of Tennessee, Knoxville,

Assistant Editor Atlantic Council Digital Forensics Research Lab, Washington DC

Chief International Security Officer, Armenian IT company.

Ex-Head of the Anti-Cybercrime Unit, Armenian Police / Head of Hi-Tech Crime Division, Main Department of Combating Organised Crime, Police of Republic of Armenia.

Political Scientist, University of Nevada, Las Vegas, Caucasus and Eurasia specialism.

Project Manager, Cybercrime Project Office, Council of Europe.

Sociologist Yerevan State University, co-author Independence Generation report, Armenia.

Vice President of the Internet Society of Armenia / Secretary of the Internet Governance Council of Armenia.

Appendix: Professional titles of expert interviewees.