UNIVERSITY OF WINCHESTER

Department of Policing, Criminology and Forensics and
Department of Social Sciences

Policy Brief: Tackling the Growth of Cybercrime in Developing and Emerging Nations

Prof Tim Hall (tim.hall@winchester.ac.uk) **and Dr Ulrike Ziemer** (ulrike.ziemer@winchester.ac.uk)

Summary of Research

Cybercriminals are disproportionately concentrated in a small number of nations, such as China, Russia, Romania and Nigeria. Cybercrime often arises where young people are computer literate but find opportunities in the legitimate economy hard to come by. It develops particularly in nations where this occurs alongside corruption, organised crime, materialism, geopolitical tensions and poor internal cybercrime policing and legislation. It has been argued that in such nations, cybercrime can be widely viewed as less criminal than other forms of crime. These are issues that particularly face some developing and emerging nations.

It is often assumed that nations that display these characteristics will inevitably be high cybercrime nations. However, this is not necessarily always so. Very little research has been conducted in nations that display these characteristics, but where cybercrime remains low or limited. Potentially we are missing lessons that might help prevent the growth of cybercrime elsewhere.

Armenia is a former Soviet nation which is adjacent to the recognized high cybercrime nations of Georgia and Turkey. Whilst it displays many of the characteristics of other high cybercrime nations, Armenia has not itself been identified as a high cybercrime nation. This research explores the reasons for this and what lessons we might learn that can be applied in the fight against cybercrime.

Types of Cybercrime

Many types of cybercrime exist that display very different motivations. Economically motivated cybercrimes includes hacking, phishing, online fraud, romance scams and blackmail. Geopolitically motivated cybercrimes include cyber espionage, terrorism and hate speech. Psychologically motivated cybercrimes include cyber stalking, bullying and revenge pornography.

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

Key Findings

- Economically motivated cybercrime originating from Armenia, despite some growth since 2010, remains low compared to surrounding nations. One expert interviewed in 2021 argued: "We still view Armenia as a low crime country in terms of cyber".
- Many instances of geopolitically motivated cybercrimes, both from abroad targeting Armenians and originating within Armenia and targeting foreign nationals and institutions, have been recognized.
- The majority of young Armenians surveyed (70.7 percent) reported being a victim of cybercrime. Over half reported being a victim of online misinformation, and over 40 percent reported being a victim of online hate speech. Over half of the cybercrime victims surveyed reported being victims of more than one form of cybercrime.
- The young people surveyed also commonly encountered cybercrime when they were online. Online misinformation and hate speech were the most commonly encountered forms of cybercrime.
- Many young people surveyed felt that the cybercrime they encountered. or were victims of, originated beyond, rather than from within, Armenia. Less than a third felt that overall Armenia was a high cybercrime country.
- Young people in Armenia overwhelmingly condemned cybercrime. Less than 9 percent of young people surveyed showed some agreement with the statement 'I think cybercriminals are less 'criminal' than people who commit crimes in the real world'. This compared to almost 80 percent who disagreed to some extent. Our results show that economically and geopolitically motivated cybercrime does not enjoy widespread social acceptance amongst young people in Armenia.

Key Findings (cont.)

- This research shows that widely held views of some regions, such as Eastern Europe and the former Soviet Union, as containing only high cybercrime nations is a simplification that hides some significant differences between nations.

IT Development and Cybercrime in Armenia

Armenia's IT sector plays an important role in preventing the growth of cybercrime there. This sector has grown rapidly since 2000 as a result of government policy and investment from Armenians overseas. This has created a high demand for people with advanced computer skills and provides legitimate, well-paid opportunities for young, computer literate Armenians. There is little incentive, then, for young, skilled Armenians to turn to economically motivated cybercrime. One expert interviewed in 2021 argued: "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".

Policy Recommendations

- Discussions of cyber-threats and anti-cybercrime policies should not target whole regions in blanket ways. This carries the danger of stigmatising some nations that pose relatively limited cyber threats. Anti-cybercrime policies and discussions should reflect the very different experiences of and attitudes towards cybercrime within developing and emerging nations.
- When talking about potential cybercrime threat nations the majority of attention has been focused on cybercrime perpetrators. More attention should be paid to understanding and promoting the experiences of the many victims of cybercrime within developing and emerging nations.
- Whilst it has often been assumed that cybercrime enjoys widespread social acceptance in some regions, there is very little direct evidence to support this. More attention should be focused on highlighting widespread social condemnation of cybercrime in developing and emerging nations.
- The experiences of victims of cybercrime in developing and emerging nations, and instances of widespread social condemnation of cybercrime, might inform the development of popular anti-cybercrime movements there, similar to anti-corruption campaigns in some developing nations.
- IT development can occur in developing and emerging nations that share characteristics of high cybercrime nations, such as high levels of poverty, without inevitably leading to a growth in cybercrime. Jobs in this sector should be sufficient in number to absorb the pool of suitably skilled workers, well-paid and free from corruption, if they are to effectively divert young people from cybercrime.

This briefing is based on the following publications:

- Hall, T. and Ziemer, U. (2023) 'Exploring the interactions between poverty, IT development and cybercrime: an Armenia case study', *Journal of Cyber Policy*, 7, 3: 353-374 Open Access: Full article: Exploring the relationship between IT development, poverty and cybercrime: an Armenia case study (tandfonline.com)
- Hall, T. and Ziemer, U. (forthcoming) 'Online deviance in Post-Soviet space: victimisation, perceptions and social attitudes amongst young people in Armenia' (Copy available from researchers)