Centre for
Global Cooperation Research

Briefing on the occasion of the 37th Käte Hamburger Lecture „Inside the Business of Cybercrime: Trust and Cooperation among Cybercriminals" , 3rd November 2020

Briefing

Cybercrime

Keywords: Anonymity, child pornography, corruption, Covid-19, cryptocurrency, cyberwar, darknet, doxing, fraud, hacking-for-hire, hacktivism, organized crime, platform, ransomware, swatting

Same same but different: crime in cyberspace

'Cybercrime' is used as an umbrella term and includes a variety of crimes enabled by or dependent on cyber-capabilities of the perpetrators. Their motivations are not essentially different from those in the offline-world: malicious, personal, political, profit-driven. Obviously the network infrastructure provides tools that make a difference: in speed, systemic refinement, seemless (borderless) communication and a new understanding of what distance means in those operations. Supposed anonymity unleashes specific energies. But how do cybercriminals cooperate?

Criminal conduct at one's fingertips has its role models. Early hacker individuals and groups established a reputation for targeting secret service and military units. As online markets developed financial institutions, for instance, were forced to hire attackers as so-called 'pentesters', regardless of their affiliations, and thus, effectively, also employed undercover FBI agents. These blurry lines between crime and its legal counterparts came under scrutiny by researchers such as Jonathan Lusthaus, who delved into these networks, conducting extensive interviews with law enforcement officers, undercover agents, and cybercriminals (Lusthaus 2018). His work reveals the very fine-grained mechanisms of cooperation in this emerging industry.

Lately, cybercrime has proven to be more profitable than the global trade of illegal drugs. Consulting and operating, cybercriminal crews and markets are on the payroll of regular legal companies and state actors. Increasingly, civil society organizations like *Transparency International* or *Citizen Lab*, a Canadian NGO, are monitoring those blurred lines and demanding an ethical standard for data management and ownership. On 26 Oct 2020 it was reported that the confidential treatment records of tens of thousands of psychotherapy patients in Finland have been hacked and leaked, in part, online. Patients were blackmailed for a payment of 200€ in Bitcoin to prevent publication of their data. In the eyes of advanced cybercriminals this may sound rather simple and crude. But it testifies that in cybercrime—by and large—there are no Robin Hoods either. Different but same same.

Definitions

Crimes are behaviors criminalized by legal systems

Cybercrime is the use of computers or other electronic devices via information systems such as organizational networks or the internet to facilitate illegal behaviors. (Samuel C. McQuade)

Distinction in law enforcement between cyber-enabled and cyber-dependent crimes

4 types

cyber-trespass: crossing boundaries (hacking)

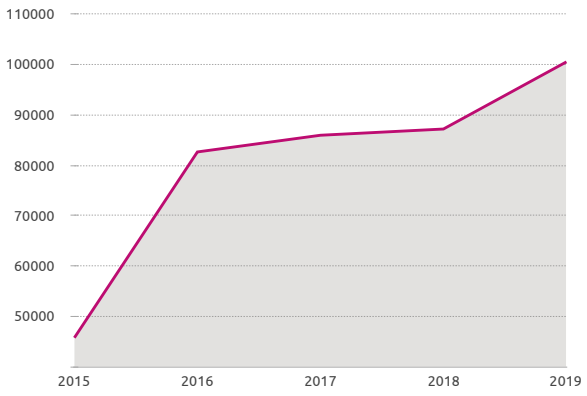
cyber-deceptions and thefts (money, IP)

cyber-pornography

cyber-violence: stalking, inciting violence, hate speech

(David S. Wall)

100.514 reported cybercrime cases in Germany in 2019



GCR21 - Data Source: BKA 2020a

Headlines

Law enforcement and cyber security

Germany's National Cyber Defense Center (NCAZ) was established in 2010 and coordinated by the BSI (Federal Office for Information Security). This coordinating role switched to the National Criminal Policy Office (BKA) in 2020. The BKA is the main actor when it comes to law enforcement in the field of cybercrime. Its annual report details trends, targets and techniques of cybercriminals. The state of Bavaria established its own Cyber-Allianz-Zentrum Bayern (CAZ) at its intelligence agency. The BKA tends to model cybercrime along its established structure combating terrorism (Joint Counter Terrorism Center, GTAZ). Europol has coordinated on the European level with its Cybercrime Centre (EC3) since 2013. The challenge to coordinate between those agencies—and its questionable efficiency—is acknowledged by many.

300 billion passwords worldwide
= 300 billion potential threats

$600 billion lost annually due to cybercrime worldwide
= almost 1% of global GDP

GCR21 - Data Sources: Cybersecurity Ventures, McAfee

Cybercrime and Covid-19

The Covid-19 pandemic motivated a broad spectrum of cybercriminal activities. Phishing mails and websites nudged people, who had applied for state financial aid, toward website clones, collecting contact and financial data. Others threatened to publish supposed abuse of those aids and offered remorseful repayment. But in contrast to subsidy fraud, according to the BKA, the damage caused by cybercrime-related activities remained low. Prices of items in the darknet increased with the pandemic. Transborder trade was partly avoided. The offline world shutdown had its effect on cybercrime. Vaccines and Covid-19-related medication are on offer. An increase of the national data traffic by 10% during 'pandemic' spring (Germany) simplified DDoS-attacks. Applications of ransomware targeting health organizations increased and likely constitutes a persistent threat. Video conference platforms were exploited without any major repercussions so far.

Organized sexual abuse

While AI and content moderation are effective against abusive networks, detections like the ones recently in Germany, which included the discovery of an extraordinary amount of material, are shocking for investigators and the public. Under lockdown conditions, the child is even increasingly exposed to spending time with their abuser and less in the position to report the abuse to someone or to get it noticed by others. Different cultural notions of pedophilia and computer-generated material, such as the so-called Japanese *lolicon* contribute to the difficulty of tracking and preventing the sharing of such content beyond borders. Pedophile groups perform specific tests for new members. These involve making original pictures available and face-to-face-meetings with members. This 'display crime' becomes the novice's admission ticket.

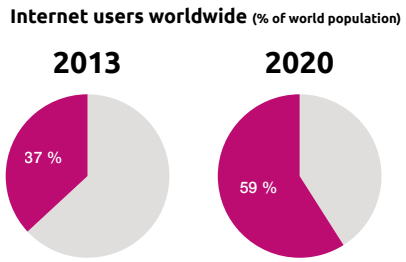
Topics

Cybercrime as a service

Division of labour is advanced in the cybercrime industry. What is sometimes called a 'firm', may be seen as time- based projects. Masterminds hire personnel for specific tasks and buy the appropriate tools. Platforms and hosts provide an eco-system, where specific coding services and strategies are exercised. But there is an element of the real world in cybercrime: cashout operations transfer money via ATM machines and shipments of goods have to be picked up ('runners' or 'drops' do this service). Enforcement techniques applied to partners of such a project can be also hired (DDoS, doxing, swatting).

Citizen Data

The commodification of personal data brings to the fore a contenstation that is driven by economic interests of companies and the regulatory governance of states. Cybercriminal trade in data finds its market here. Credit card data were the outstanding top item in cybercrime since even before its professionalization as an industry around the millennium. Crime follows money and industrial development. Driver data from automobiles, health and voter data offer new fields. Social Media struggles with data breaches and exploitation from quite different actors, starting from an individual, peer group level to firms like Cambridge Analytica, aggregating huge amounts of data for commercial profit, sold to state and non-state actors. Outsourcing of surveillance to platforms like Amazon, Huawei and Palantir results in private companies executing sovereign actions. A buyer's market is established and - part of - cybercrime could go semi-legal.



GCR21 - Data Source: statista

Cybercrime law and defamation

Egypt's President Abdel Fattah Al-Sisi ratified the country's first 'cybercrime law' in August 2018. The law is considered to be the first legislation of its kind in Egypt. Article 7, which focuses on regulating censorship, gives the authorities the right to censor Egyptian-based or foreign websites spreading propaganda that may threaten national security or the national economy. Decisions can be appealed before the criminal court within seven days of censorship of the website, according to article 8 of the law. Our first Briefing on Online Defamation already pointed out that cyber-law in a number of countries criminalizes what is seen by human rights advocates as an instance of free speech and legitimate forms of societal debate.

Techniques

Trust your anonymous partner?

Jonathan Lusthaus in his seminal study (Lusthaus 2018) asks how trust could be built inside cybercrime, where even more than in traditional crime, anonymity and distance make proof and enforcement measures difficult. But he found that appearance, performance and reputation are an asset carefully styled, modified and enhanced by those actors, because business opportunities are quite dependent on those factors. Trust is enhanced over time, repetition is a strategy. There are entrance fees for new contacts and supercookies, to prove one's identity. Display crimes confirm skills and commitment. Cyber-specific enforcement techniques (B2B) include SIM-swapping, doxing, swatting (sending police to your home). And agents? Whereas Russian hackers erected a language barrier consciously, this made broken English difficult to judge as either pretense or native (Russian).

Platforms and groups

Cybercrime departed from a scene of hackers and coders and in its early phase shows an element of playful competition, political activism and Robin Hoodism. The credit card fraud business with some spectacular hacks turned the scene from a bio-sphere of 'crews' into a business direction. Division of labour and roles and professionalization established an industry from about the turn of the millennium on. Platforms like CarderPlanet (Odessa 2001, founder 'Script' aka Dmitri Golubov later became a member of parliament in Kiev) and ShadowCrew established a lasting role model: code east - cashout west. Dark Market, established 2005, was administered by Keith Mucharsky, an undercover agent for the FBI. Small groups tend to use platforms as a marketplace to make occasional contacts and deals. But the work is done on a different layer—in project crews, or as 'Script' labeled it once: in 'dens of wolves'.

The 'roof': interfaces of cybercrime

Cybercriminals may give the impression of being mercenaries in cyberspace ('hacking-for-hire'). Their skills make them attractive and approachable for quite different projects. The history of hacking almost starts with this ambivalence: compare white hats like Steve Jobs and Steve Wozniak with black hats Kevin Poulsen and Kevin Mitnik. As mercenaries coding cybercriminals can be protected by organized crime firms or corrupt politicians. In the very special Russian environment, It is common to search for protection. This is called a *krysha* ('roof'). 'Protection by officials appears much more regularly than protection by organized crime groups' (Lusthaus 2018: 181).

The dark side of cooperation

In 2012, when the Centre for Global Cooperation started research in Duisburg, global cooperation enjoyed a positive connotation. Global cooperation was associated with multi-lateral political deliberation of a new kind, taking a common global horizon into consideration and asking the question, how constructive endeavors among members of the international community could be fostered.

With cybercrime we focus on the other darker pole of this vision. Transborder cooperation and coordination is one of the older assets of crime. Crime, including profit-driven crime, has a keen interest in borders, scrutinizing ways to exclusively access them and also to hide behind. Cooperation is a dual-use item. And if we believe that the world is not black and white, we should say: multiple-use. Cybercrime therefore is clearly a topic for global cooperation research.

'Cybercrime a tragedy'

For Lusthaus, the scene he studied for such a long time. is a 'tragedy', as he notes at the end of his book. Besides the career criminals there are those 'intelligent, capable and driven individuals', who invest all talent and energy and ultimately 'all this effort is destructive rather than constructive.' And he imagines what would happen, 'if this talent pool could be diverted away from cybercrime and into legitimate industry' (2018: 199). This question is even more convincing if combined with a look into current demand for global innovation, preservation and change. People who are able to hack into US Customs and Border Protection and the Antwerp port system or coordinate complex transborder cashout operations would focus on big data, energy distribution or DDoS-attack those killing the Amazon forest. But this would be cybercriminal again, right?

Pushing the dark side further down? The Travel Rule for Crypto

The Financial Action Task Force (FATF), an intergovernmental organization to combat money laundering, observes the 'travel rule' of money which means that banks must have detailed customer information about both parties in transactions in excess of $3,000. This 'Travel Rule' was officially extended to 'virtual asset services providers' (VASPs) in June 2020 which requires VASPs, such as crypto exchanges, to collect the names of both transaction senders and receivers, as well as the national IDs of the former. Malcolm Campbell-Verduyn foresees that 'the FATF's approach is dividing the crypto-ecosystem into dual infrastructures. One more consolidated and centralized infrastructure enables compliance with the Travel Rule and its identification requirements. But a more decentralized and privacy-centric infrastructure is pushed further into gray markets and the shadows of the dark web.'

Tackling Cybercrime - international conventions and organizations

UNO
Resolution adopted by the General Assembly on 27 December 2019
74/247 Countering the use of information and communications technologies for criminal purposes

Resolution 26/4 of 26 May 2017
Commission on Crime Prevention and Criminal Justice

UN General Assembly resolution 55/25 of 15 November 2000
United Nations Convention against Transnational Organized Crime (the Palermo Convention)

UN Sources
UNODC cybercrime repository
Usefull: Database of Legislation (member states)
Expandable: Case Law Database (member states)

UNODC 2015
Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children

European Union

EU Cybersecurity Strategy 2017

The EU Cybersecurity Act
Regulation (EU) 2019/881 of 17 April 2019
Infographic

The European Union Agency for Cybersecurity (ENISA)
Regulation (EC) No 460/2004, updated under Regulation (EU) No 526/2013

Cybercrime Centre (EC3) within Europol (since 2013)
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Budapest Convention on Cybercrime
(adopted by the Council of Europe at its 109th Session on 8 November 2001)

Sources

Bendiek, Annegret, Bossong, Raphael, and Schulze, Matthias (2017). The EU's Revised Cybersecurity Strategy, SWP Comments 47, November.

Bill Marczak e.a. (2018). The Kingdom Came to Canada. How Saudi-Linked Digital Espionage Reached Canadian Soil, 1st October.

Bundeskriminalamt (BKA) (2020a). *Cybercrime, Bundeslagebild* 2019 (Stand: September 2020). Wiesbaden.

Bundeskriminalamt (BKA) (2020b). *Cybercrime, Sonderauswertung Cybercrime in Zeiten der Corona-Epidemie* (Stand: September 2020). Wiesbaden.

Campbell-Verduyn, Malcolm and Hütten, Moritz (2020). Is the Travel Rule Good or Bad for Crypto? Both, *coindesk*, 27 June

Kennedy, Jay, Holt, Thomas and Cheng, Betty (2019). Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking, *Journal of Crime and Justice*, 42:5, 632–645.

Krebs, Brian (2014). *Spam Nation: The Inside Story of Organized Cybercrime – From Global Epidemic to Your Front Door* (Naperville, Il. : Sourcebooks.

Krempl, Stefan (2020). 'Amazon, Huawei, Palantir: Warnung vor Überwachungs-Outsourcing bei der Polizei', *Heise online*, 05.07.2020.

Legality of child pornography by country (wikimedia commons).

Lusthaus, Jonathan (2018). *Industry of Anonymity. Inside the Business of Cybercrime*, Cambridge, Mass./London: Harvard University Press.

MacQuade, Samuel C. (2006). *Understanding and Managing Cybercrime*, Boston: Allyn and Bacon, 16.

Pieper, Oliver (2019). 'Child sex abuse at German campsite: How authorities failed the victims', *Deutsche Welle (dw.com)*, 05.09.2019, Permalink https://p.dw.com/p/3L5Gg.

Poulsen, Kevin (2011). *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*, New York: Crown.

Samir, Mohamed (2018). 'Al-Sisi ratifies cybercrime law regulating web content, ISP surveillance', *Daily News Egypt*, 18 August.

'Shocking' hack of psychotherapy records in Finland affects thousands, AFP in Helsinki / The Guardian, 26 Oct 2020

Sztompka, Piotr (1999). *Trust: A Sociological Theory*, Cambridge: Cambridge University Press.

Wall, David S. (2007). *Cybercrime. The Transformation of Crime in the Information Age*, Cambridge: Polity.

Centre for
Global Cooperation Research

Käte Hamburger Kolleg / Centre for Global Cooperation Research (KHK/GCR21)
A Central Research Institute of the Unversity of Duisburg-Essen
Director: Sigrid Quack | Co-Directors: Tobias Debiel, Dirk Messner, Jan Aart Scholte
Schifferstraße 44, 47059 Duisburg
Phone: +49 (0)203 379 5230 Fax: +49 (0)203 379 5276
E-Mail: info@gcr21.uni-due.de

Briefing 2/2020 - GCR21 Public Relations – editor: Martin Wolf – picture credit: Shutterstock
Recherche: Victoria Derrien, Janine Herbert, Milena Gaede (charts)