Cybercrime in Austria – Methods and Strategies on Fighting Online Crime

Mag. Judith Grohmann (Donau Universität Krems)

Introduction

More than ever, postindustrial societies and highly developed countries are taking advantage of cyberspace in their quest for technological, economic, social, cultural, scientific, and political development. Digital infrastructures are becoming the backbone of a successful economy, a vibrant research community, a transparent state, and free society.[1] Public administration no longer relies exclusively on traditional channels of service delivery but considers the internet indispensable for reaching out to the general public. Citizens, on the other hand, must have confidence that their data will be received by addressees fast and reliably.

This broad reliance of governments and citizens on information technology has given rise to new forms of criminal activity, as anyone who uses the computer and the internet is at risk of encountering online criminality and cybercrime. Indeed, cyber enables criminals to commit crimes in both cyber- and physical space. For example, a criminal may use information technology to monitor the behavior of people to know when they are out of town so that he may rob their house. Often, perpetrators do not need highly technical equipment, as crimes may be committed via relatively simple devices such as smartphones. With new trends and threats constantly emerging, the police must therefore keep pace with new technologies, to understand the possibilities they create for criminals, and how they can be used as tools for fighting cybercrime.

Per Interpol, "Cyberattacks know no borders and evolve at a fast pace while the Internet also facilitates a range of more traditional crimes."[2] Additionally, the European Consumer

[1] *Austrian Cyber Security Strategy 2013*, of the Federal Chancellery, Federal Ministry of Internal Affairs, Federal Ministry of Foreign Affairs, Federal Ministry of Defense, Introduction, p. 4, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

[2] Interpol Homepage: https://www.interpol.int/Crimes/Cybercrime.

Center Austria, which has been created to assist European consumers in cases of cross-border complaints, notes that "cybercrime is a booming field and no safety door or alarm system can stop it, because it has found completely new ways to attack our privacy. The common opinion that computer systems can be fully secured is now changing—there is no 100 percent safety."[3] Indeed, total eradication of cybercrime is impossible, leaving us with just mitigation and response preparedness, the goal being to get far enough ahead that we are not always just reacting, but anticipating, planning, and responding with well-thought-out actions.

In this article, we first discuss the concept of cybercrime in some detail, first by providing an overview of what it *threatens*, i.e., why its existence should be of concern to those interested in the efficient functioning of modern society. We then examine out the difficulties encountered in defining the term, analysing the differences between cybercrime and traditional crime, and briefly surveying the multiple forms cybercrime can take. From there, we move to a discussion of the Austrian case, discussing first the overall statistics pointing to a severe increase in cybercrime in Austria, followed by two mini case-studies of hacking efforts with detrimental effects for Austrian security. This is followed by an examination of mitigation efforts undertaken by Austrian authorities.

Cyberspace: *What* Is Under Threat

Cyberspace has developed over the years "into a vital area of activity for the state, the economy, science, and society."[4] Most obviously, it is a rapidly growing *space for information and communication*. The number of people using email grew from 3.9 billion worldwide to 4.04 billion in 2020, while approximately 2.4 billion emails are sent every minute and 306.4 billion e-mails are sent each day.[5] Google searches count more than 3.5 billion per day.[6]

[3] European Consumer Center Austria, May 29, 2013, "Cybercrime: New Brochure of the ECC and VKI," https://europakonsument.at/en/page/cybercrime.
[4] *Austrian Cyber Security Strategy 2013*.
[5] "The Surprising Reality of How Many Emails Are Sent Per Day," https://techjury.net/stats-about/how-many-emails-are-sent-per-day#gref.
[6] "Google Search Statistics – Internet Live Stats," https://www.internetlivestats.com/google-search-statistics/.

Furthermore, cyberspace functions as a *space for social interaction*. While more than 4.3 billion people use the internet, social media users specifically have passed the 3.8 billion mark.[7] Facebook is the largest social networking site in the world, with four hundred new users signing up every minute.[8] Worldwide, there were over 2.5 billion monthly active users as of December 2019, an 8 percent increase over 2018.[9] At the same time, other social media companies are also continuing to expand, with TikTok as only one up and coming competitor to challenge Facebook recently. The app hit 1.5 billion downloads in November 2019 and was the third most-downloaded nongaming app of that year, outperforming both Facebook and Instagram.[10]

Third, cyberspace has taken on critical importance as an *economic and trade space*, developing into a marketplace of strategic importance in a relatively short period of time. Global e-commerce sales volume jumped from $572 billion in 2012 to $29 trillion in 2017.[11] The implications for this in terms of how companies utilize behavioral data are staggering. In her eponymous book, Shoshana Zuboff writes,

> Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as "machine intelligence," and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call *behavioural futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behaviour.[12]

[7] "Digital Trends 2020: Every Single Stat You Need to Know about the Internet," https://thenextweb.com/podium/2020/01/30/digital-trends-2020-every-single-stat-you-need-to-know-about-the-internet/.

[8] "Wild and Interesting Facebook Statistics and Facts (2020)," https://kinsta.com/blog/facebook-statistics/.

[9] https://zephoria.com/top-15-valuable-facebook-statistics/, January 29, 2020.

[10] "Sheryl Sandberg Said She Worries about TikTok," *Business Insider*, January 29, 2020, https://www.businessinsider.com/sheryl-sandberg-said-she-worries-about-tiktok-2020-2.

[11] UNCTAD, "PRESS RELEASE: Global E-Commerce Sales Surged to $29 trillion," March 29, 2019, https://unctad.org/en/pages/PressRelease.aspx?OriginalVersionID=505.

[12] John Naughton, "Shoshana Zubov Age of Survaillance Capitalism," *The Guardian*, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

Fourth, cyberspace serves as *space for political participation*, with important implications for the relationship between a government and the society it governs. Globally, states are increasinigly capapble of reaching out to their citizens through e-government, offering easy access to popular federal services. This may include, but is not limited to, permitting citizens to download forms, make appointments, send in applications, and make payments online all via a single portal.[13] While this raises concerns about foreign governments tampering with elections and thereby posing challenges to democratic processes,[14] digital forms of interaction open up new opportunities for political participation and political expression.

Finally, *the function of cyberspace as an information space is closely related to another function, that of "control space."* New technologies permit actors to monitor, operate and maintain practically all infrastructures of the transport, economic, industrial, health, and educational sectors. In part, this is aided by the development of the so-called Internet of Things (IoT), in which the number of internet-connected devices continues to grow, even if not at rates predicted in the early heady days of the phenomenon. In 2012, an IBM forecast predicted 1 trillion connected devices by 2016; the true total as of 2020 is likely "somewhere between … 6.4 billion (excluding smartphones, tablets, and computers), and … 17.6 billion (with all such devices included)."[15] The sector continues to grow, with the number of devices connected to the internet, including machines, sensors, and cameras, growing at a steady pace. In 2019, the International Data Corporation (IDC) estimated that by 2025 there will be 41.6 billion

[13] OECD, Observatory of Public Sector Innovation, "National One-Stop Shop for Government Services and Information," Ministry of Public Administration, 2015-2018, https://www.oecd.org/governance/observatory-public-sector-innovation/innovations/page/nationalone-stopshopforgovernmentservicesandinformation.htm

[14] Uri Friedman, *The Atlantic*, "Here's What Foreign Election Interference Will Look Like in 2020," August 2019, https://www.theatlantic.com/politics/archive/2019/08/foreign-election-interference-united-states/595741/.

[15] Amy Nordrum, "*The Internet of Fewer Things – Early Predictions of 50 Billion Connected Devices by 2020 Are Being Scaled Back*," September 23, 2016, www.spectrum.iee.org.

connected IoT devices, or “things,” generating 79.4 zettabytes (ZB) of data a year.[16] Already, IoT has advanced well beyond science fiction status, steadily infiltrating factories, homes, and businesses all over the world.[17] IoT is more and more offering advanced connectivity of devices, systems, and services that goes well beyond machine-to-machine communications. The interconnection of all of these devices will result in increased automation in nearly all fields, leading to increases in efficiency, accuracy, and economic benefit as well as reduced human intervention.[18] While the benefits are enormous, the increase of IoT can also lead to Industrial Control Systems (ICS) security vulnerabilities, particularly since research from IBM shows that 81 percent of companies do not have an operational technology (OT)-specific security incident response plan in place. Potential attacks against against ICS and supervisory control and data acquisition (SCADA) are especially alarming, presenting a real security threat to vital production facilities that could have a devastating impact on energy, utilities, transportation, and other systems that touch all of our lives.[19]

Cybercrime

Term and definition

Cybercrime, also called computer crime, maybe defined as the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Especially through the internet, it has grown in importance as the computer has become central to commerce, entertainment, and government, and represents an extension of existing criminal behavior

[16] Press Release, *Marketwatch*, June 18, 2019, https://www.marketwatch.com/press-release/the-growth-in-connected-iot-devices-is-expected-to-generate-794zb-of-data-in-2025-according-to-a-new-idc-forecast-2019-06-18?mod=mw_quote_news.

[17] “The Most Powerful Internet of Things (IoT) Companies to Watch,” *Computerworld*, https://www.computerworld.com/article/3412287/the-most-powerful-internet-of-things-iot-companies-to-watch.html.

[18] “Reap the Benefits of IoT without Compromising SCADA Security,” *Security Boulevard*, February 2020, https://securityboulevard.com/2020/02/reap-the-benefits-of-iot-without-compromising-scada-security/.

[19] Ibid.

alongside some novel illegal practices.[20] Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the internet. Indeed, in this digital age, our virtual identities are essential elements of everyday life: we are more or less a "bundle of numbers and identifiers in multiple computer databases owned by governments and corporations." Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.[21]

The difficulty countries globally face in combatting cybercrime is compounded by the fact that there is no commonly agreed upon definition of the phenomenon, hindering the development of legislation to effectively address all activities that fall under the "cybercrime" umbrella. Furthermore, there are no cyberborders between countries, meaning that international cybercrimes often challenge the effectiveness of domestic and international law and law enforcement. Precisely because existing laws in many countries are not tailored to deal with cybercrime, criminals increasingly conduct crimes on the internet in order to take advantages of the less severe punishments or difficulties of being traced. Certainly, governments and industries across the globe have gradually realized the colossal threats of cybercrime to economic and political security and public interests. National regulatory frameworks have an important role to play in cybercrime prevention, both with respect to the private sector in general and service providers in particular. Nearly half the world's countries have passed data protection laws specifying requirements for the protection and use of personal data. Some of these regimes include specific requirements for internet service providers and other electronic communications providers.[22]

[20] "Cybercrime," Encyclopaedia Britannica online, https://www.britannica.com/topic/cybercrime.
[21] Ibid.
[22] United Nations Office on Drugs and Crime – Vienna (UNODOC), "Comprehensive Study on Cybercrime" February 2013, page xxvii,

However, complexity in types and forms of cybercrime increases the difficulty of fighting back, suggesting the need for increased international cooperation, a call that governments have increasingly taken up in recent years. For example, the Council of Europe Convention of 23 November 2001,[23] also called the Budapest Convention on Cybercrime, is a Council of Europe convention open for signature by its member states and nonmember states that participated in its elaboration and for accession by other nonmember states. It is the first international agreement on crime committed via the internet or other computer networks to deal with topics like "infringements of copyright, computer related fraud, child pornography, and violations of network security."[24] The agreement thus represents the international endeavor to establish uniform and legal regulations to combat cybercrime and facilitate international cooperation in this area.

Also in Europe, with Regulation (EU) 2016/679 of the European Parliament and of the Council, the European Union's General Data Protection Regulation (GDPR) regulates the processing (by individuals, by companies, or by organizations) of personal data relating to individuals in the EU. The rules do not apply to data processed by an individual for purely personal reasons or as part of activities carried out in one's home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside of the personal sphere, for sociocultural or financial activities, for example, then the data protection law must be respected.[25]

Cybercrime and traditional criminal activity

https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf.

[23] Glossary of the "official website of the European Union:" https://ec.europa.eu/home-affairs/e-library/glossary/budapest-convention-cybercrime_en.

[24] Council of Europe, Details of Treaty No. 185: "Convention on Cybercrime," Budapest, November 23, 3001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[25] Official Homepage of the European Union, "Law"/ "What Does the General Data Protection Regulation (GDPR) Govern?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en.

Combatting cybercrime is further complicated by the ambiguous relationship between it and traditional criminal activity. While “cybercrime” involves digital computers in the commitment of an offence, the technology alone is insufficient to distinguish these types of activities from traditional crimes. Generally speaking, criminals do not need a computer to commit a fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone’s privacy. All those activities existed before the “cyber” prefix became omnipresent; in this way, cybercrime (especially when it involves the internet) often represents an extension of existing criminal behavior alongside some novel illegal activities that have been made possible by the presence of these technologies. Further complicating matters, “today’s cybercriminal is not necessarily an IT-specialist.”[26] Crucially, cybercrime differs from traditional crime in that it knows no physical or geographic boundaries and can be conducted with less effort, greater ease, and at much greater speed than the latter, although to be sure this depends on the type of cybercrime and the type of “traditional” crime it is being compared to.[27]

The risks and threats

Cyber risks and threats confronting users range from operating errors to massive attacks by state and nonstate actors using cyberspace as a venue for their activities; they may also involve military operations. Cybercrime, whether in the form of identity fraud, cyberattacks with the intent of harming an enemy state, or misuse of the internet for extremist purposes are serious new challenges facing all the stakeholders affected, requiring broad cooperation of governmental and nongovernmental bodies at the national and international levels.[28]

Cybercrime – The Austrian Case

[26] Interview with Mr. Erhard Friessnik, current Head of the Cybercrime Competence Center C4 at the Federal Austrian Ministry of Internal Affairs.

[27] Marie-Helen Maras, *Computer Forensics: Cybercriminals, Laws and Evidence*, Jones & Bartlett Learning 2014.

[28] Austrian Cyber Security Strategy 2013, p. 6.

Austrian understandings of cyberspace – ICT as a target, ICT as a tool

In Austria, about three quarters of the population uses the internet regularly, and half of this group does so on a daily basis. The economy depends increasingly on effective digital infrastructures with regard to its technological development and the efficiency of internal procedures.[29] All of this puts Austria, its citizens and government, at risk from cybercrime, a fact that has led the government to implement mitigating policies. The goal of the Austrian ministry of the interior is to observe and analyze development in this area, to investigate the perpetrators, and to protect internet users with the knowledge gained during the investigations and international analysis meetings and debriefings with relevant experts within and outside of the European Union. Furthermore, the Ministry of the Interior seeks to constantly build up appropriate expertise and develop new strategies and to adapt these—often only short-lived—policies to the cybercrime situation in Austria.[30]

The government of Austria understands that the cyber security of Austria, the EU, and the entire community of nations is interconnected very closely; a corollary understanding is that intensive cooperation based on solidarity at the European and international level is required to ensure cyber security.[31] Indeed, ensuring cyber security in national and international cyberspace has become one of Austria's top priorities and a common challenge for the state, national business, and society. With the *Austrian Strategy for Cyber Security,* the Federal Government of Austria rolled out on March 20, 2013, a comprehensive and proactive concept for the protection of cyberspace and the people who move around within it. The *Strategy* has since then served as the basis of government policy in this field.[32] At the same time, it should be noted that Austria's EU membership mandates that the country utilize the above-mentioned

[29] Ibid., p. 4.
[30] Interview with Erhard Friessnik.
[31] *Austrian Cyber Security Strategy 2013*, p. 7.
[32] Austrian Chancellery, "Bundeskanzleramt"/Themen/Cyber-Sicherheit, https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html.

GDPR as a tool in fighting cybercrime, meaning that whenever an individual in Austria uses personal data outside of the personal sphere, the data protection law must be applied.[33]

As a cross-cutting issue that requires a broad approach, Austria treats the fight against cybercrime both as one of the core tasks of the Austrian criminal police at Federal Criminal Police Office (BKA)[34] and an area that falls under the purview of the Austrian security authorities at the Ministry of Internal Affairs.[35] Generally, the relevant Austrian authorities understand cybercrime in two senses, namely, the narrow and the broad. In the Austrian context, cybercrime in the narrower sense includes criminal acts that a) involve attacks on data or computer systems and b) are committed using information and communication technology (ICT).[36] These offenses are directed against the networks themselves or against devices, services or data in these networks,[37] for example, data corruption, hacking, or DDoS attacks. Offenses that belong to "cybercrime in the narrower sense" can be found in the following Law Paragraphs in the Austrian Criminal Code[38]:

- § 118a StGB Illegal access to a computer system
- § 119 StGB Violation of telecommunications secrecy
- § 119a StGB Misuse of data
- § 126a Data corruption
- § 126b StGB Disruption of the functionality of a computer system
- § 126c StGB Misuse of computer programs or access data
- § Section 148a Fraudulent misuse of data processing
- § 225a StGB Data falsification

[33] Official Homepage of the European Union, "Law/ What Does the General Data Protection Regulation (GDPR) govern?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en.

[34] The "Bundeskriminalamt" (abbreviation = BKA).

[35] The "Bundesministerium für Inneres" (abbreviation = BMI)

[36] *Lagebericht Cybercrime 2018*, also known as "Cybercrime-Report des Bundeskriminalamtes 2018," chapter 2.1, Kategorisierung des Begriffs/Cybercrime (Vienna: n.d, 2018), p. 9.

[37] Ibid.

[38] Österreichisches Strafgesetzbuch (StGB), https://www.jusline.at/gesetz/stgb.

By "cybercrime in a broader sense" are understood crimes in which information and communication technology is used as a direct tool for planning, preparing, and executing conventional criminal offenses, such as fraud, drug trafficking in the darknet, pornographic representations of minors on the internet, cybergrooming, or cyberbullying.[39]

Austria's membership within the EU means that the authorities must also account for other distinctions, emanating from EU regulations. For instance, in 2018 the European Union Agency for Law Enforcement Cooperation ("Europol") differentiated between *cyber-dependent* crimes[40] and *cyber-enabled* crimes.[41] The key distinction between these categories is the role of ICT in the offence—whether it is the target of the offence or part of the *modus operandi*[42] of the offender.[43] When ICT is the target, the cybercrime negatively affects the confidentiality, integrity, and/or availability of computer data or systems.[44] Alternatively, when it is part of the modus operandi, ICT is used to commit crimes with other targets, often in furtherance of "traditional" criminal ends (robbery, blackmail, etc.).

Cybercrime in Austria: General trends and specific case studies

The number of offenses committed by cybercrime "in the narrower sense" rose across Austria from 2,630 in the year 2016 to 3,546 in the year 2017, as reported by the BKA and corresponding to "an increase of 34.8 percentage points compared to the previous year."[45] On the one hand, the situation seems to be deteriorating—the number of such offenses reported for 2018 was about 19, 627, an increase of 16.8 compared to 2017. On the other hand, the capacity of the state to deal with them has also been rising: the number of solved crimes rose by 13.3

[39] *Lagebericht Cybercrime 2018*, p. 10.

[40] I.e., "any crime that can only be committed using computers, computer networks or other forms of information communication technology." From Mike McGuire and Samantha Dowling, *Cybercrime: A Review of the Evidence*, *Research report 75, Summary of key findings and implications,* UK Home Office Research Report 75, October 2013, p. 4; Europol, 2018, p. 15.

[41] I.e., traditional crimes facilitated by the internet and digital technologies.

[42] Or M.O.; i.e., method of operation.

[43] UNODC, *E4J University Module series: Cybercrime*, 2013, p. 15.

[44] Ibid.

[45] Österreich-oe24.at, "Cybercrime bei uns stark am Vormarsch," March 2018, https://www.oe24.at/digital/Cybercrime-in-Oesterreich-stark-am-Vormarsch/349177951.

percent in 2108, from 6,470 in 2017 to 7,332.[46] At the same time, if one looks at Austrian cases of cybercrime in the "broader sense," these too have been increasing, especially in the areas of forged documents, cases of blackmail by ransomware, pornographic representations of minors on the internet, and fraud generally speaking.

Taken together, according to the Police Crime Statistics (PKS), the number of suspects in the area of cybercrime increased in 2018 to 7,980, which signifies an increase of 7.1 percent from 2017. In terms of gender distribution, 70.1 percent (5,591) of the suspects were male and 29.9 percent (2,389) were female. The age distribution of possible offenders showed that the majority of (3,547) is between 25 and 39 years old, followed by those over 40 (1,896) and from 21 to 24 years old (1,110).[47] It should be noted that the highest rates of increase in criminality generally in Austria have been in the area of cybercrime, apparently reflecting the ongoing shift of classic forms of crime into the digital world.[48]

If we look at the situation for 2019, surveys published by the BKA for the first half of 2019 show a striking increase in internet crime in Austria over the period from January to June of that year, registering a change of 51 percent from 2018.[49] The decisive factor for the increase in quantity seems to be a spike in internet frauds, which were registered in 8,187 police reports, an increase of 32.3 percent from the comparison period. Further parsing the numbers, it appears that cybercrime "in the narrow sense" increased by 61.6 percent in 2019, including but not limited to cyber attacks on third-party devices, data theft, and trade in stolen identities on the Darknet. These trends are only forecast to increase in the coming years.[50] Finally, the

[46] Based on the *Austrian Cybercrime Report 2019 –Developments, phenomena and priorities* (*Lagebericht Cybercrime 2019 – Entwicklungen, Phänomene und Schwerpunkte*), p. 17, https://bundeskriminalamt.at/306/files/Cybercrime_Report_18_web.pdf.
[47] Based on the *Austrian Cybercrime Report 2019 – Developments, Phenomena and Priorities* (*Lagebericht Cybercrime 2019 – Entwicklungen, Phänomene und Schwerpunkte*), p. 17, https://bundeskriminalamt.at/306/files/Cybercrime_Report_18_web.pdf.
[48] Ibid., p. 18.
[49] "Cybercriminality in Austria Has Increased," September 12, 2019, https://www.onlinesicherheit.gv.at/service/news/470499.html.
[50] Ibid.

highest increase, of 144.9 percent, occurred in the category of “other crimes” on the internet. For some time now, common criminal acts—extortion, document forgery, money laundering, etc.—have increasingly moved to the Darknet, where criminals may also purchase malware (also referred to as “crime-as-a-service.”).[51]

Such are the broad trends, the “numbers,” as it were. In what follows, we look at two mini case studies of cybercrime in Austria, namely, two cases of hacking into governmental systems that encapsulate the extent to which cybercrime is not merely a phenomenon affecting people’s pocketbooks, but is also a problem for state/social security broadly conceived.

Hacking into the Austrian People’s party server

As technology changes, countries and their election management bodies must change how they conceive of security. Battles for the integrity of elections and for control over political parties are increasingly waged in cyberspace, and one small flaw in technology, or in the way it is used, can jeopardize an election and political parties themselves. Importantly, the increased digitization of the electoral field brings to the fore the extent to which the balance between transparency and security is perhaps the central issue in cybersecurity. While technology needs to be sufficiently opaque to bad actors, the public can quickly lose trust in any system that is a “black box” to nonexperts. Securing voting technology means more than just strong software and hardware—it also means securing the human, political, legal, and procedural aspects of an election.

Indeed, voter data is just as much of a target for malicious hacks and breaches as, say, credit card data and it is equally susceptible to poorly secured digital infrastructure. In fact, the problem has already reached a global scale. Voter data can be exposed by either a malicious hack, an accidental leak, poorly configured security settings, or the physical theft of hardware.

[51] Ibid.

Regardless of the point of exposure, compromised voter data usually includes sensitive and personally identifiable information.[52]

On September 5, 2019, the Austrian People's Party[53] reported to the media, that a "very targeted hacker attack" on the party headquarters had occurred. As a result of this incident, the "the hacker (or the hackers) got access to the systems of the political party on July 27 and had 'exfiltrated' 1.3 terabytes of data by the end of August 2019.[54] According to the People's Party, the attack was noticed "because confidential documents about the party's donations and campaign finances have been leaked to the media."[55] The party also claimed that the data "could not only have been stolen but also manipulated," although in the immediate days after the incident no evidence of manipulation was detected.[56]

In October 2019, the Austrian media reported that "the alleged hacker attack on the People's Party headquarters was apparently 'started by a server in Vienna.'" Clues initially led investigators to a club of comics fans in Vienna in the Favoriten district. However, it was reported that the club members "themselves may have been victims of the hackers."[57] Apparently, the club's server may have been hacked and used "as an attack platform against the People's Party server;" while focusing on the club, investigators "came across several suspicious IP addresses that could lead to the actual perpetrators."[58]

Over time, the magnitude of the breach became clear. In the course of parliamentary inquiries to the Austrian justice minister Clemens Jabloner and Interior Minister Wolfgang Peschorn in November 2019, it was confirmed that "463 gigabytes of data have been

[52] "Personal Data: Political Persuasion, Inside the Influence Industry's – How it Works," and "Breaches, Leaks, and Hacks: the Vulnerable Life of Voter Data": https://ourdataourselves.tacticaltech.org/posts/breaches-leaks-hacks.

[53] German: Österreichische Volkspartei (ÖVP) is a conservative and Christian-democratic political party in Austria.

[54] https://futurezone.at/netzpolitik/oevp-hack-ermittlungen-werfen-neue-fragen-auf/400636748.

[55] https://orf.at/stories/3137375/.

[56] Ibid.

[57] "ÖVP-Hackerangriff: Spur zu Comic Verein in Favoriten?", *Die Presse*, October 10, 2019.

[58] Ibid.

transferred to a French server."[59] Data was transferred between August 30 and September 1. Based on previous investigations, it was assumed that the attacker(s) changed the administrator password at least once in the internal IT network of the People's Party. As a result, authorized persons were "temporarily" locked out of the party's IT application, and the hackers were able to access the entire network on July 27.[60]

One day after the attack was reported, the public prosecutor's office in Vienna opened an investigation against "unknown perpetrators" on suspicion of unlawful access to a computer system and data damage to the detriment of the People's Party. At the time of this writing, the investigation was being carried out by the BKA and included technical experts from the Federal Office for the Protection of the Constitution and the Fight against Terrorism. So far, there have been no official indications that it was an attack by a foreign intelligence service, or that other parties were hacked to a comparable extent (or that such attempts had been made).[61]

Cyberattack on the Austrian Foreign Ministry in 2020

Late on Saturday, January 4, 2020, the Austrian government reported to the media a cyberattack at the Ministry of Foreign Affairs (MFA), noting that it was part of a pattern in which "other European countries have … been targeted for similar attacks in the past."[62] Further, the MFA let it be known that "the seriousness of the attack suggested it might have been carried out by a 'state actor'."[63] The ministry confirmed that "countermeasures" were in place while an "interagency task force reviewd the situation, and that services, such as travel information, were still available via the MFA's website.[64]

[59] "ÖVP-Hackerangriff: 463 Gigabite Daten trannsferiert," *Kurier,* November 14, 2019.
[60] Ibid.
[61] Ibid.
[62] Michael Shields and Alison Williams, "Austria Suspects Foreign State behind Cyberattack," Reuters, January 5, 2020.
[63] BBC, "'Serious Cyber-Attack' on Austria's Foreign Ministry," January 5, 2020.
[64] Shields and Williams.

The MFA was quick to put the attack in context, noting that "despite all intensive security measures, there is never 100 percent protection against cyber acttacks;[65] it also, as already mentioned, pointed out that other European governments had been similarly victimized in recent years. For example, the German government's IT network experienced a "very serious" cyberattack in March 2018. The culprit was a Russian cyber espionage group called Fancy Bear, associated with the Russian Cyber Agency GRU[66] and said to be sponsored by the Russian Government.[67] Operating since the mid-2000s, the group is thought to be responsible for cyberattacks against the White House, NATO, French Television station TV5Monde, the Democratic National Comitee, the Organization for Security and Cooperation in Europe, and the campaign of the French presidential candidate Emmanuel Macron; it was also suspected to have been involved in a similar attack on the German parliament in 2015.[68]

From these two cases, an important conclusion emerges. Namely, cyber attacks by hackers against Austria's governing institutions, here the electoral system and the Ministry of Foreign Affairs, should not be considered in isolation from processes affecting the governments of Western societies broadly speaking. Much remains to be learned, for example, about the connections between the Austrian incidents and apparent Russian interference in the US presidential election of 2016. Combatting this form of cybercrime requires cooperation on the international level, both within Europe and across the Atlantic.

Cybercrime in Austria: Mitigation Strategies

Austrian authorities have been addressing the problem in a variety of ways. In addition to intense investigative efforts on the national and international (especially European) levels, the country has launched a societal campaign for safe online behavior. Experts from the BKA

[65] BBC, "'Serious Cyber-Attack'."

[66] Lawrence Osterle, "Russia behind Fancy Bear Hacks, Claims UK Government Report," *Independent*, October 4, 2018, https://www.independent.co.uk/sport/general/athletics/fancy-bears-hacks-uk-russia-government-vladimir-putin-a8567771.html.

[67] "Fancy Bear," *Wikipedia*, https://en.wikipedia.org/wiki/Fancy_Bear.

[68] BBC, "'Serious Cyber-Attack'."

and the scientific and private sectors have strengthened cooperation within the framework of joint projects with Europeol. One notes also an increase in the use of prevention programs such as "Under.18" and "Cyber.Sicher" (Cyber.Secure). Plans are in the works for enhanced training for internet crime investigators and for setting up a central investigation team in the area of ransomware.[69]

Combatting cybercrime in Austria involves numerous structures and stakeholders, reflecting the wide range of operations falling under the "cybersecurity" umbrella; already existing processes and structures establish a higher level of coordination on both the political-strategic and operational levels. Several organizations specialize exclusively in cybersecurity—for example, on the state level, the Computer Emergency Response Team (CERT)[70]—and play an important role in cyber crisis management. These are discussed at some length below.

Organizational structure for law enforcement against cybercrime

On May 11, 2012, a Ministerial Council decision established a Cyber Security Steering Group, with a political-strategic mandate, and placed it under the leadership of the Federal Chancellery.[71] The steering group coordinates cybersecurity measures, observes and monitors the implementation of the *Austrian Cybersecurity Strategy*, prepares annual reports on cybersecurity and advises the Federal Government in related matters. Membership comprises liaison officers to the National Security Council and cybersecurity experts from the departments represented in the latter, including the Federal Chief Information Officer. The steering group also works with those government departments whose sphere of influence includes organizations and companies addressed or affected by control measures proposed by

[69] "Cybercriminality in Austria has increased," September 12, 2019, https://www.onlinesicherheit.gv.at/service/news/470499.html.

[70] The homepage of the Austrian Computer Emergency Response Team is: https://cert.at/en/home/.

[71] *Austrian Cybersecurity Strategy 2013*, p. 10.

the group; relevant cocmpanies are also consulted.[72] Furthermore, steps have been taken to coordinate existing operational structures and incorporate them into one overaching body;[73] also, a cyber crisis managemetn structure has been set up made up of representatives of the Austrian state on the one hand and operators of critical infrastructures on the other.[74]

The Austrian Cybercrime Competence Center ("C4") was established in 2011 to fight against "Computer Criminality" as a separate unit within the BKA's Assistance Services Department. The "C4" is the national and international contact point to fight cybercrime in Austria. The core is made up of highly specialized experts from the areas of electronic evidence protection and digital investigations. Organizationally, the "C4" is divided into five units, namely, "Central Tasks," "IT Evidence Preservation," "Investigations," "Development and Innovation," and a registration office. It is responsible for national and international coordination and reporting on investigations in connection with cybercrime, as well as for the electronic securing of evidence and its evaluation. The registration office acts as a point of contact for the Austrian population as well as for companies, so that rapid support can be provided and new negative phenomena can be recognized at an early stage.[75]

Notably, the "C4" is characterized by organizational adaptability, driven by the continuously changing nature of the enemy. According to the "C4"'s current head, Erhard Friessnik, "Developing a strategy is nice, however, these strategies always have to be adapted…because the strategies can be just as short-lived as the topic is." Indeed, the strategy of the department depends on the technology used by the criminals in question; operationally, this means that the first questions asked by the department when a crime has been reported are "Where does the whole thing go? Which technique does the other person/the criminal use?

[72] Ibid.
[73] Ibid.
[74] Ibid., p. 11.
[75]https://www.onlinesicherheit.gv.at/service/initiativen_und_angebote/beratung_und_sensibilisierung/71347.html.

Which techniques are…also available to the police?" To that end, the Cybercrime Competence Center is constantly building up "appropriate expertise," in the hopes that it will be able to apply it when necessary.[76]

When a cybercrime occurs, citizens have recourse to a Cybercrime Reporting Office located at the BKA.[77] This fits into the C4 strategy of "having police officers at police stations, who are knowledgeable in this area, who understand the victim, who have further understanding of the crime and who are able to interrogate the victim to get as many important informations as needed," in order for investigations to proceed efficiently.[78] According to Friessnik, while prevention is important, the cyber security mandate of the C4 is broader, allowing the task force to move "proactively" toward cases of cybercrime: "appropriate rules have been imposed for the protection of critical infrastructures. This is where the Network and Information Systems Act, the so-called NIS-directive, comes in, where certain companies are required to comply with certain security standards."[79]

Furthermore, the "C4"'s activities are actively tied into the international effort to combat cybercrime. For instance, it acts as an international hub interface for the Cyber Security Center (CSC) of the Federal Office for the Protection of the Constitution and Counterterrorism (BVT).[80] Similarly, the C4 registration office serves the European Cybercrime Center[81] (EC3) at Europol, the Interpol Digital Crime Center (IDCC), and all relevant international police departments and specialist organizations as an information resource and contact point.[82]

[76] Interview with Erhard Friessnik.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] BVT = Bundesamt für Verfassungsschutz und Terrorismusbekämpfung.
[81] Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses. and governments from online crime. Since its establishment, EC3 has been involved in dozens of high-profile operations and hundreds on-the-spot operational-support deployments resulting in hundreds of arrests; it has analysed hundreds of thousands of files, the vast majority of which have proven to be malicious. See About Europol/European Cybercrime Centre - EC3: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
[82] *Austrian Cybercrime Report 2018 – Developments, Phenomena, and Priorities*, p. 11, https://www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf.

Despite its constitutional "perpetual neutrality" with regard to NATO, Austria (and therefore the "C4") works with the NATO Cooperative Cyber Defence Centre of Excellence located in Talinn.

Areas of focus

In addition to dealing with crimes related to crypto currency and the Darknet, in recent years, Austria's efforts at combatting cybercrime have focused on several major areas:

1. Data leaks

A data leak is the intentional or unintentional release of secure or private/confidential information into an untrusted environment. For example, e-mail addresses with associated passwords from hacked companies and portal operators are becoming increasingly available for free, not only in underground forums of the Darknet but also on the internet. Previously installed apps containing malware are also employed for data and identity misuse. Finally, over the past few years large collections of leaked data have been compiled from various sources and offered again in a bundled form, with the data usually coming from attacks on various devices and applications.[83] Finally, poorly secured web portals or company employee-and-customer platforms offer points of attack.

Austrian investigations, both locally and with international support, have focused on identifying leaked data sets available on the web and matching them to potential victims. As a preventive protective measure, the "C4" registration office and investigators were, in 2018, able to notify and alert almost 100,000 potentially injured parties.[84]

2. Distributed Denial-of-Service attacks

A denial-of-service attack—also called DoS attack—is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by

[83] *Austrian Cybercrime Report 2018*, p. 21.

[84] Ibid.

temporarily or indefinitely disrupting services of a host connected to the internet. In 2018 Austria chaired the Council of the European Union for the third time, from July 1 to December 31, 2018. Based on the experience of other countries which had previously held the EU presidency, the Austrian investigative authorities paid particular attention to combating in advance a particularly pernicious form of DoS, the so-called "DDoS," or Distributed Denial-of-Service attack. The latter is defined in relevant Austrian terminology as "a malicious attempt to disrupt normal traffic of a targeted server, service or network, by overwhelming the target or its surrounding infrastructure with a flood of internet traffic;" these types of attacks "achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic."[85]

For the purpose of preventing DDoS attacks in advance during its European presidency, the "C4" participated in the international European Multidisciplinary Platform Against Criminal Threats projects (EMPACT) and also in operational missions at the Joint Cybercrime Action Taskforce (J-CAT) at Europol in the Netherlands.[86] Already in April 2018 one of the largest service providers for "DDoS" attacks, *webstresser.org*, was removed from the internet via the coordination of J-CAT with the operational action "Power Off." Among other things, this successful international operation enabled the increase in DDoS attacks to be kept low during the presidency, successfully avoiding the sharp increase that characterized the experience of other countries in previous years.[87]

3. Ransomware

Ransomeware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it, unless a ransom is paid. Austria has taken on this particular threat very strongly in recent years; indeed, "the Austrians have acquired a

[85] Ibid.
[86] Ibid.
[87] Ibid.

pioneering role throughout Europe."[88] This is because Austria was one of the first countries to "centralize ransomware investigation, at the Federal Criminal Police Office. And with that, all the notifications received in Austria were summarized in the Federal Criminal Police Office, which categorized and analyzed accordingly and was able to identify (recognize) groups of offenders to a certain extent."[89]

Known as the SOKO Clavis unit, the team of investigators at C4 tasked with combatting ransomware has shown remarkable success, particularly in mitigating the extortion Trojans *NotPetya* and *Wanna Cry*. While these were a major problem in 2017, extorting hundreds of thousands of computers worldwide that year, by 2018 at least in Austria the cases were on the wane, as SOKO Clavis "managed to investigate several accused people and suspects linked to large ransomware variants, some of which were responsible for more than a hundred million euros of damage."[90]

Conclusion

As early as March 2013, Austria's top intelligence officials cautioned that cyberattacks and digital spying are the top threat to national security, eclipsing even terrorism. In the last seven years, Austria has found its role, especially in cybercrime forensic science and is in a position to help other countries, especially those within the European community. Yet, challenges remain. For example, according to Erhard Friessnik,"The speed of an information and communication technical forensic investigation always depends on the circumstances….If you have a device today, that is unencrypted and open, you usually have a result in a few hours. With a highly encrypted device and with the right measures, it may only be the case that you get partial results from these forensics."[91] Complicating matters, "The customer thinks: I want

[88] Interview with Erhard Friessnik.
[89] Ibid.
[90] *Austrian Cybercrime Report 2018*, p. 22.
[91] Interview with Erhard Friessnik.

my system to be secure. No matter what happens. And only I have access and nobody else. The one who has evil in mind sees this much more strictly. Logical. He doesn't want to be caught."[92]

In Friessnik's assessment, other circumstances make it difficult for forensic technicians to conduct their investigations in Austria (and elsewhere), namely, the overarching interests of the tech companies: "Well-known manufacturers, like Microsoft, Apple, etc., prioritize customer satisfaction, because they don't get any money from the security authorities, while the customer pays a manufacturer money for his good product." And because "the manufacturer needs the customer in the first place, he will primarily represent the interests of the customer and only afterwards, the interests of the authorities. [Therefore] the manufacturer makes his systems even more secure, […] making forensic access ever more difficult."[93]

As mentioned, despite the increasingly professional and efficient efforts of the Austrian investigators pursuing cybercrime, the numbers of crimes in this area continues to rise significantly in the country. The international aspect of this type of criminality and the existence of perpetrator networks are jointly responsible for this phenomenon, despite the best efforts of the Austrian authorities. At the same time, the continually expanding expertise of "C4" and other stakeholders working to mitigate cybercrime in Austria, as well as their participation in relevant international committees and projects, suggest that the criminals have not yet definitively won the battle, as an ongoing strong global network of law enforcement agencies makes its resources available to the defenders of Austrian law and order.

[92]Ibid.

[93] Ibid.