CS1800 Situation Analysis

Attached is the **Cybercrime** Situation Analysis for CS1800.

Some things to remember:

- **Think multidimensionally**: cyber policy impacts many different issues, and it is important to identify potential risks and opportunities in your analysis. Consider the strengths and weaknesses of several possible responses and select the optimal response.
- **Engage the scenario**: Assume that the situation which we have provided you is plausible. At the same time, think critically about the information that you have been provided and its origins.
- **Consider interests:** Organizations have a broad and diverse set of interests. How might your decision impact other interests which your organization would like to secure? If you choose one course of action, would a different office at your organization reject your approach? Be sure to be able to justify your response as strongly as possible.
- **Think holistically:** It is important to also consider not just your interests, but *all* parties' interests, including states and non-state actors.

What you are responsible for:

1. A brief, informal oral presentation by your group in section. There are no requirements for using visual materials, nor are there requirements for how many members of your group must speak. Expect to outline your course of action for roughly five, but no more than ten, minutes.

2. Engaging in a brief Q&A from your classmates and your TAs afterwards. We will be assessing the degree to which you have prepared justifications for your course of action.

3. A brief, informal one-page summary of your proposed plan of action to be emailed to your TAs at 11:59 PM the day before your section. Formatting is not especially important – we just want a record of your approach for evaluation purposes. Bullet points are acceptable in this assignment. No bibliography is required.

4. Filling out a peer evaluation after your presentation, during which you will have the opportunity to inform the HTAs about whether all members of your group contributed fairly to your group assignment.

Included in this brief:

1. A letter from the Secretary of State's office asking for your recommendation.

2. A brief guide to U.S. foreign policy tools.

3. An article published in *Slate* discussing the Russian government's approach to cybercrime.

Disclaimer: While some situation analyses for CS1800 are entirely fictional, others are based on real events. You should think about the "date" of your scenario and discount any events that have occurred in the real world after that date.

DATE: February 22, 2020

You are a team of foreign service officers (FSOs) in the Department of State and have been asked by the Secretary of State to draft a plan for the Office of the Coordinator for Cyber Issues (OCCI) regarding a recent instance of transborder cybercrime targeting U.S. businesses.

Secretary of State Pompeo is determining the best course of action after a recent, major string of cybercrimes against American businesses. While the legal consequences of the attack are, of course, significant, there are also major dimensions of international relations that must be addressed by your office.

On February 15, 2020, seven medium-sized and major U.S businesses and organizations reported to the FBI that they had fallen victim to a new ransomware worm, apparently named "CryptoCry" by its engineer. The worm encrypted the business' servers with a very strong AES 256-bit encryption scheme and demanded a ransom of $300,000 (USD) for access to the decryption key. Five of the businesses paid the ransom, while two have yet to do so.

CryptoCry appears to have intentionally targeted businesses that had a strong incentive to pay the ransom as quickly as possible: three are hospitals, two are municipal transport systems, one is a local water treatment plant, and one business coordinates agricultural shipments around the U.S. It is worth noting that the Department of State is only aware of businesses which reported the ransomware attack to the FBI; it is possible that dozens of other businesses were targeted by CryptoCry, but have chosen not to disclose the attack due to perceived financial disincentives.

The National Security Agency (NSA) has high confidence in its attribution of CryptoCry. According to an NSA report issued on February 17, 2020, CryptoCry was developed and deployed by Igor Olegovich Turashev (a.k.a. "GrimVision"), a Russian national operating from Moscow. NSA has concluded that Turashev is also responsible for a string of minor cyberattacks in 2016 and 2017 which targeted businesses in Ukraine. NSA has further informed us that in 2018, Turashev received the equivalent of $30,000 (USD) from Russian intelligence services for his freelance hacking work. In Russia, it is common for the intelligence services to hire civilian hackers to complement their existing cyber forces. We do not, however, have any indication that the CryptoCry attack was a state-sponsored effort.

Although the U.S. and Russia do not have an extradition treaty, on February 18, 2020, we filed a request with the government of Russia to consider arresting Turshev under Russia's nominal cybercrime statutes. Moscow responded on February 19 by informing the Department of State that they have no knowledge of any Russian nationals by Turashev's name and recommend that the U.S. arrest our Treasury Secretary for his sanctions on Russian oligarchs.

Please draft a response for the Secretary of State as soon as possible that outlines the best course of action to effectively punish this crime and deter similar crimes in the future. We are attaching a matrix of U.S. foreign policy tools and options for your reference.

Sanctions Working Group,
State Department Advisory Committee on International Economic Policy

U.S. Foreign Policy Tools
An Illustrative Matrix of Selected Options

KEY:
IFI : International Financial Institution
OPIC : Overseas Private Investment Corporation
EXIM : Export-Import Bank
TDA : Trade and Development Agency
GSM : General Sales Manager (USDA Export Credits)

	Friendly, Persuasive		Hostile, Coercive	
DIPLOMATIC (Executive)	• Embassy Open/Expand • Ambassador: Accredit • Visas: Liberalize • Landing Rights: Extend/Expand • Intl Org: Support Membership/ • Support Position • Intl Conf: Support Spons/particip	• Communiqué: Friendly • State Visits: Support • Senior Officials Exchange: Support • Hostile Neighbors/Opposition: Minimize Contact	• Embassy: Reduce Staff • Ambassador: Recall for Consults • Visas: Restrict to targeted groups • Landing Rights: Restrict • Binatl Comms: Pare Back • Intl Org: Oppose memb/position • Intl Confs: Oppose spons/particip • Communiqué: Hostile • State Visits: Oppose • Sr. Officials Exchange: Restrict	• Embassy Close • Ambassador: Withdraw • Visas: Suspend • Landing Rights: Suspend • Binatl Comms: Suspend • Intl Orgs: Urge Exclusion • Intl Confs: Urge Exclusion • State Visit: Cancel • Sr. Officials Exchange: Cancel • Hostile Neigh/Opposit: Expand Contact
POLITICAL (Executive & Legislative)	**LEGISLATIVE** • Resolutions: Friendly • CODELS: Increase • NBD: Increase Funding • Intl Parliamentary Orgs: Support Participation/Position • Opposition: Minimize Contact • Arms Transactions: Support	**EXECUTIVE** • Proclamation: Friendly • State/Local Exchanges: Sister City Agreements, State Offices, Overseas - Support	**LEGISLATIVE** • Resolutions: Hostile • CODELS: Fact-Finding Missions • NBD: Restrict Funding • Intl Parliamentary Orgs: Oppose • Opposition: Increase Contact • Arms: Cancel Trans/Boycott	**EXECUTIVE** • Proclamation: Hostile • Opposition: Host Visit
CULTURAL (Executive & Legislative)	• Aggressive Broadcasts: Decrease/Suspend • Academic Exchange: Establish/Expand • Intl Athletic Events: Support Participation/Support Sponsorship • Entertainment/Cultural Tours: Support Participation/Sponsorship	• Peace Corps: Expand • Public: Exchange: Establish/Expand • Intl Cultural Organizations: Support memb. • Scientific Coop: Establish/Expand Internet Sites: Expand	• Aggressive Broadcasts: Increase • Academic Exch: Restrict • Intl Athletic Events; Oppose Participation/Sponsorship • Entertainment/Cultural Tours: Oppose Participation/Sponsorship • Peace Corps: Restrict • Publication Exch: Restrict • Intl Cult Orgs: Oppose memb. • Scientific Cooperation: Restrict	• Academic Exch: Suspend • Intl Athletic Events: Urge Exclusion • Entertainment/Cultural Tours: Ban from US Entry/Urge Exclusion • Peace Corps: Suspend • Publication Exch: Suspend • Intl Cultural Orgs: Urge Suspension • Scientific Coop: Suspend
ECONOMIC (Executive & Legislative)	• Debt Rescheduling: Permit/ Liberalize Terms • Pref Tariff Treatment: Expand • Reg Trade Agrmts: Permit Particip • Trade Credits: Expand • Investment: Expand Promotion • Bus Contacts: Encourage • Trade Missions: Expand • OPIC/EXIM/TDA: Open/Expand	• Trade Controls: Liberalize • Double Tax Agreement: Negotiate • Tax Treaty: Negotiate • IFIs: Support membership/position • Financial Controls: Relax • Assets: Release • Postal Cooperation: Expand • Aid/Technical Assistance: Increase	• Debt: Tighten Terms • Investment: Restrict Promotion • Business Contacts: Discourage • Trade Missions: Pare • OPIC/EXIM/IDA: Restrict on Targeted Basis • Trade Controls: Limited (commodity/product based) • IFIs: Oppose membership/position • Financial Controls: Increase • Aid/Technical Assistance: Restrict	• Debt: Suspend • Pref Tariff Treatment: Suspend • Regional Trade Agreements: Suspend Participation • Trade Credits: Restrict • Investment: Ban • Business Contacts: Ban • Trade Missions: Suspend • OPIC/EXIM/TDA: Suspend • Trade Controls: Expand • Trade Embargo • Double Tax Agreement: Suspend • Tax Treaty: Suspend • IFIs: Urge Exclusion • Assets: Freeze • Postal Cooperation: Suspend • Aid/Technical Assistance: Suspend • G7 Sanctions Group: Activate
MILITARY (Executive: Legislative Consultation)	• Training (IMET/E-IMET): increase • Officer Exchange: Increase • Military Coop (Joint exercises/ training/tech coop); Increase • Port Visits: Increase • Confidence-building Measures: Increase	• Peacekeeping Forces: Maintain • Coop w/Hostile Neighbors/ Opposition: Restrict • Local Maneuvers: Restrict	• Peacekeeping Forces: Maintain • Coop w/Hostile Neighbors/ Opposition: Restrict • Local Maneuvers: Restrict	• Training: Suspend • Officer Exchange: Suspend • Military Cooperation: Suspend • Port Visits: Suspend • Conf. Bldg Measures: Suspend • Peacekeeping: Withdraw • Coop w/Neighbors/Opp: Increase • Local Maneuvers: Increase • Show of Force • Act of War

ESCHERIAN GEOMETRIC IMPOSSIBILITIES

future tense

Why the Russian Government Turns a Blind Eye to Cybercriminals

As long as they target victims in other countries, that is.

By TIM MAURER
FEB 02, 2018 • 12:02 PM

Photo illustration by Slate. Photos by Thinkstock.

Future Tense is a partnership of Slate, New America, and Arizona State University that examines emerging technologies, public policy, and society.

Posting photos of your luxury cars on social media is probably not the best idea if you are a hacker committing cybercrime. Yet that's exactly what Karim Baratov did. It is therefore not surprising that the 22-year-old Canadian got caught and pleaded guilty in November to being involved in the Yahoo hack, the biggest data breach ever (to date). That cybercrime is lucrative isn't news, of course, but the Baratov case stands out because the indictment details his relationship with the FSB, a Russian intelligence service on the other side of the planet.

Baratov, the son of Kazakh immigrants, was paid by two FSB officials as part of a larger operation targeting Yahoo that also involved Alexsey Belan, who had already been on the FBI's Cyber's Most Wanted list but managed to avoid being extradited to the U.S. The two were used as cyber proxies: intermediaries who conducted an offensive cyber operation benefiting the Russian intelligence agency. How states organize and structure these proxy relationships differs from state to state, but Baratov and Belan's story provides insight into proxy relationships between the Russian state and hackers. What we now know largely affirms rumors that had been floating around for the past two decades.

Former Soviet states boast citizens with highly developed technical skills, thanks to university departments in math, engineering, and computer science that have ranked among the world's best for decades. It is the result of systematic literacy campaigns after the 1917 revolution, with the campaigns boosting the literacy rate from 22 percent at the beginning of the 20th century to full literacy by the time the Soviet Union collapsed. While states that used to be part of the Soviet Union still rank among the world's most literate and educated societies, unemployment has risen, and the economy has not been able to absorb this technically skilled workforce. The economic crash in 1998 exacerbated the problem. It's estimated that only 50 percent of Russian software companies survived the downturn. Around the same time, cybercrime started to become a growing and lucrative business.

The same challenges persist today. For example, someone in his 20s holding a cybersecurity job in the Ukrainian government today would earn roughly $3,000 a year. And while Samsung has one of its largest R&D centers in Kiev, the private IT industry is neither large nor attractive enough to absorb the available skilled labor. As Alexei Borodin, a hacker, put it, “People think: ‘I’ve got no money, a strong education and law enforcement’s weak. Why not earn a bit on the side?’ ” In sum, there is no labor shortage in the region when it comes to information technology and hacking, but the legitimate industry is not big enough to absorb all of the labor, and government salaries of a few thousand dollars a year pale in comparison to reports of thousands or millions made in the latest cyber heist. At the turn of the 21st century, several hundred Russians had already participated in hacking competitions such as the one organized by Hackzone.ru, and hacker magazines had a monthly circulation in the tens of thousands. By 2014, the Moscow-based cybersecurity company Group-IB estimated the size of the cybercrime market in Russia alone to be $2.3 billion. Since hackers take great care not to target people within the area of the former Soviet Union but focus on victims in the United States and Europe, it is not surprising that few arrests are made by Russian law enforcement agencies. The Russian government often does not respond to requests for assistance from foreign law enforcement agencies and frequently protests when Russian nationals are arrested abroad. For example, when Vladimir Drinkman, a Russian national wanted for committing cybercrime, was arrested while vacationing in Amsterdam in 2012, the Russian government tried to block the U.S. government’s extradition request by filing its own extradition request, thereby at least delaying prosecution.

"Russian law enforcement and the FSB in particular have a very good idea of what is going on and they are monitoring it, but as long as the fraud is restricted to other parts of the world they don't care," said cybercrime expert Misha Glenny. Another indication that the Russian government can effectively enforce the law if it so chooses is the fact that malware used by Russian and east European cybercriminals is often designed so that it "purposefully avoids infecting computers if the program detects the potential victim is a native resident." For example, one site pays people for installing its adware and spyware on machines in dozens of countries but points out on its website that "[w]e do not purchase Russian and CIS [Russian Commonwealth] traffic." When Russian hackers do target victims in Russia, Moscow's response is swift and harsh. In 2012, eight men were arrested by Russian police after stealing some $4 million from several dozen banks, including some in Russia. According to security blogger Brian Krebs, "Russian police released a video showing one of the suspects loudly weeping in the moments following a morning raid on his home."

The state's tolerance of criminal activities, or rather people abusing state authority for private gain, can become even more convoluted. Take the example of Dmitry Ivanovich Golubov (Dmytro Holubov), a 33-year-old Ukrainian national from Odessa. Wanted by U.S. law enforcement as a top cybercriminal accused of credit-card fraud, Golubov was briefly imprisoned in 2005 "until two influential Ukrainian politicians convinced a judge to toss out the case," according to a former FBI agent who investigated the case. After founding the Internet Party of Ukraine in 2007, Golubov has been a member of the Ukrainian Parliament since 2014. The reason he pursued a seat in the Ukrainian Parliament? According to Krebs, "[G]ain[ing] a seat in

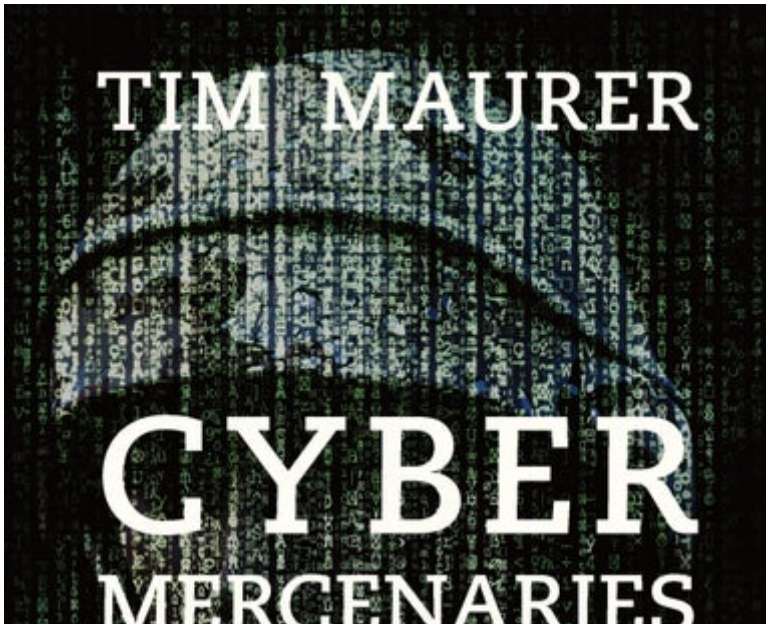
the Ukrainian government … would grant him automatic immunity from prosecution for criminal activities under Ukrainian law."

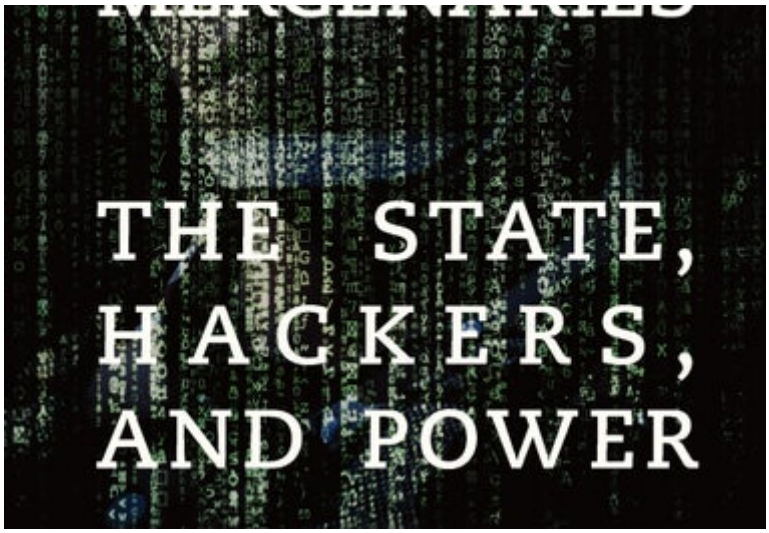
A similar example is Roman Valerevich Seleznev, a 33-year-old Russian national and the son of Valery Seleznev, a member of the Russian Parliament and the ultranationalist Liberal Democratic Party. He was convicted by a U.S. federal jury of financial cybercrime that reaped millions in profit. The Secret Service arrested him while he was on vacation in the Maldives rather than trying to work with the Russian government to arrest him—perhaps because of his family connections and certainly because of Russian law enforcement agencies' general reluctance to cooperate. Seleznev's arrest caused significant tension between Moscow and Washington. The Russian Ministry of Foreign Affairs accused the U.S. government of having "kidnapped" Seleznev when it arrested him as he was boarding a plane in the Maldives and transferred him to Guam and then to Seattle. (In court in the United States, Seleznev's defense tried to challenge the circumstances of the arrest but was unsuccessful.)

The Russian Ministry of Foreign Affairs maintains that "the practice of detaining Russian citizens following U.S. requests to third countries all over the world is a legal abuse and violation of internationally recognised proceedings." When the U.S. government used a fake job interview to trick a suspect, Vasily Gorshkov, into traveling to the United States, and U.S. law enforcement agents accessed Gorshkov's computer in Russia, the Russian government therefore also protested. Such action, they said, "violated a 1997 agreement that mandates 'investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.' " In the weeks leading up to a December 2015 visit by Secretary of State John Kerry, the ministry demanded that "U.S. law enforcement authorities stop the hunt for Russian citizens in other countries."

Such sanctioning can turn into more proactive interest from the government. In some cases, entering a proxy relationship allows a nonstate actor to avoid arrest, as described by Oleg Gordievsky, the former head of the KGB office in London, who said in 1998 that "[t]here are organised groups of

hackers tied to the FSB and pro-Chechen sites have been hacked into by such groups. … One man I know, who was caught committing a cybercrime, was given the choice of either prison or cooperation with the FSB and he went along." In such cases, in return for their cooperation, the hackers not only avoid prison but are actively defended by the Russian government. Cybersecurity experts Alexander Klimburg and Heli Tiirmaa-Klaar described one such case in which the Tomsk FSB office described malicious activity against pro-Chechen websites in 2002–2004 as being legal. This system of the FSB turning hackers into proxies for internal and external offensive cyber operations was also reaffirmed by Sergei Pokrovsky, the editor of the hacking magazine Khaker, and Vasilyev, a convicted hacker and the head of the Moscow Civil Hacking School.





That brings us back to the Yahoo hack. In March, the U.S. government unsealed an indictment that offered unprecedented insight into the relationship between FSB officials and cybercriminals. It reinforced previous anecdotal evidence and offered new details as to why and how this proxy relationship was beneficial to all parties involved. The indictment listed three Russian citizens living in Russia, including two FSB officers as well as a Canadian national residing in Canada, accusing them of cybercrime and espionage primarily targeting Yahoo starting in January 2014. The two FSB officers were Igor Anatolyevich Sushchin, 43, and Dmitry Aleksandrovich Dokuchaev, 33. Both belonged to the FSB's Center for Information Security. (Sushchin was Dokuchaev's superior.) They were accused of targeting the online accounts of specific individuals, including journalists and government officials in the United States and Russia, as well as private sector officials in the financial, transportation, and other sectors. To achieve their objectives, they worked with two cybercriminals: the Russian citizen Alexsey Alexseyevich Belan, also known as "Magg," 29, and the Canadian, Karim Baratov, also known as "Kay," "Karim Taloverov," and "Karim Akehmet Tokbergenov," 22. According to the indictment, the two FSB officers "protected, directed, facilitated and paid [the] criminal hackers to collect information through computer intrusions in the U.S. and elsewhere."

What was the benefit for Belan and Baratov to work with the FSB? For Belan, it was avoiding a U.S. prison. He had been indicted in the United States in 2012 and 2013 for various cybercrimes and was arrested in Europe in June 2013. However, he managed to escape to Russia before being extradited. In spite of Interpol issuing a Red Notice for his arrest in July 2013 and the FBI adding him to its Cyber's Most Wanted criminals list in November 2013, the Russian government refused to arrest him. The indictment reveals that the Russian government instead "used him to gain unauthorized access to Yahoo's network." In addition to avoiding having to face charges in a U.S. court, Belan benefited from information shared by the FSB officers that helped him "avoid detection by U.S. and other law enforcement agencies outside Russia, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers." Finally, Sushchin and Dokuchaev turned a blind eye to Belan's enriching himself on the side: In addition to providing them with access to Yahoo accounts, "Belan used his access to steal financial information such as gift card and credit card numbers from webmail accounts; to gain access to more than 30 million accounts whose contacts were then stolen to facilitate a spam campaign; and to earn commissions from fraudulently redirecting a subset of Yahoo's search engine traffic."

For Baratov, residing in Canada, the incentive was money. Whereas Sushchin and Dokuchaev used Belan to gain access to targets' Yahoo accounts, they asked Baratov to gain access to a target's accounts with other providers and paid a bounty in return. According to the indictment, "When Baratov successfully obtained unauthorized access to a victim's account, he notified Dokuchaev and provided evidence of that access. He then demanded payment—generally approximately U.S. $100—via online payment services. Once Dokuchaev sent Baratov a payment, Baratov provided Dokuchaev with valid, illicitly obtained account credentials." Baratov was arrested in Canada on March 14.

The use of cyber proxies in the former Soviet Union today tells us a lot more about the political realities in those countries than just the role that hackers play. Even 25 years after the Soviet Union's collapse, it is clear that the economic situation remains dire enough to provide fertile ground for criminal activity—activity that in the digital age can be far removed from the victim and allow the perpetrator to avoid arrest and often even detection. The amount of money at stake has also made it attractive for corrupt local officials to work with those technically savvy enough to pull off cyber heist after cyber heist. The new possibilities enabled by offensive cyber operations and those able to conduct them have also drawn the attention of intelligence agencies. The combination of economic hardship, relative impunity, and high reward has created an environment in which malicious activity is permitted as long as certain rules are followed, primarily finding victims abroad rather than at home.

The availability of highly skilled and technically well-versed individuals also presents a pool of potential proxies that can be mobilized at a moment's notice. Often, people will mobilize themselves and take political action in support of the government, as has happened in Estonia in 2007 and in Ukraine since 2014. Governments differ in their ability to catalyze such activity and the extent to which they are in a position to merely endorse, orchestrate, or actively direct their outcomes. In countries where public institutions and the state's ability to exercise control have deteriorated, it is an uphill battle to break the increasingly entrenched incentive structures reinforcing existing proxy relationships. Meanwhile, the controversy over law enforcement cooperation, including mutual legal assistance and extradition, shows the limits of international cooperation and external influence. The phenomenon described in this chapter is therefore a cautionary tale of the potential pitfalls when a state significantly weakens or collapses and the consequences that will reverberate for decades to come.

Extracts from Cyber Mercenaries: The State, Hackers, and Power *by Tim Maurer. © Tim Maurer 2018, published by Cambridge University Press, reproduced with permission*

Cybersecurity Russia