OpenAccessPub

Journal of Advanced Forensic Sciences

ISSN: 2692-5915

DOI: 10.14302/issn.2692-5915.jafs-22-4131

Review Article

Freely Available Online

The Computer Crimes of Vasiliy Gorshkov and Alexey Ivanov

Donald L. Buresh, Ph.D., J.D., LL.M.[1,*]

[1]Morgan State University

Corresponding author:

Donald L. Buresh, Ph.D., J.D., LL.M. Morgan State University.

Keywords:

Alexey Ivanov, American exceptionalism, Computer Fraud and Abuse Act, Extra-Territorial Computer Searches, Special Prosecutor Robert Mueller, Vasiliy Gorshkov

Received: Mar 11, 2022

Accepted: Mar 22, 2022

Published: Mar 23, 2022

Abstract

The purpose of this essay was to document the cybercrimes of Vasiliy Gorshkov and Alexey Ivanov, starting from their humble beginnings in Chelyabinsk, Russia to their convictions for conspiracy, violations of the Computer Fraud and Abuse Act, and other federal crimes. The paper outlines the history of these two individuals, describing the circumstances under which they were arrested and prosecuted. The essay concludes by observing that the mainstream media characterized Gorshkov and Ivanov as villainous Russian hackers, whereas in reality, they were would-be Russian entrepreneurs attempting to earn their fortune by illicit means.

Introduction

The purpose of this paper is to analyze the computer crimes of Vasiliy Gorshkov and Alexey Ivanov using a slight modification of the Valeriano and Maness criteria[1] as what was accomplished by the author in a previous article regarding the Estonian cyber incident[2]. The analysis focuses on answering the following four questions[3]

1. How did the crimes committed by Gorshkov and Ivanov come about?
2. What were the legal, national, and international implications of the crimes committed by Gorshkov and Ivanov?
3. What was the impact of the crimes committed by Gorshkov and Ivanov? and
4. What was the reaction to the crimes committed by Gorshkov and Ivanov on the national and international levels?

There are four actors involved in the of the crimes committed by Gorshkov and Ivanov–Vasiliy Gorshkov, Alexey Ivanov, the Federal Bureau of Investigation (FBI), and the victims of Gorshkov's and Ivanov's crimes. The paper does not address the actions of the victims of Gorshkov's and Ivanov's crimes, nor does it consider in any great depth the relationship between Gorshkov and Ivanov. Rather, it concentrates on the relationship between Gorshkov and the FBI, and Ivanov and the FBI. The paper con-

cludes by observing that it was entirely appropriate for Gorshkov and Ivanov to be prosecuted in the United States. Finally, it is entirely possible that Gorshkov, Ivanov, or both were involved in providing technical assistance to Special Prosecutor Robert Mueller indicted 12 Russian hackers, each one individually named in the complaint[4].

How Did the Crimes Committed by Gorshkov and Ivanov Come About?

In this section, the facts of Gorshkov's and Ivanov's crimes are outlined. Gorshkov's case is discussed in some detail. Finally, the Ivanov's case is outlined, describing the charges and the results of the court proceedings.

A Short History about Gorshkov and Ivanov

The mainstream media is alive these days with tales of Russian hacking of American companies, political parties, and the federal government[5]. These hackers have been involved in some extremely large cybercrimes. For example, in 2014, Russian Federal Security Service (FSB) officers Dmitry Dokuchaev and Igor Sushchin were convicted of hacking over one billion Yahoo! Accounts[6]. Another example of Russian hacking occurred when Sasha Panin hacked over one million computer systems and stole credit card and bank account information[7].

In 1999 and 2000, Vasiliy Gorshkov and Alexey Ivanov were two young Russians actively engaged in cybercrime[8]. Gorshkov and Ivanov grew up in Chelyabinsk, one of the most polluted places on the planet due to a mysterious explosion in a nuclear-bomb-making factory in the 1950s[9]. Gorshkov was a troubled youth even though he was a computer whiz because played with the computers in his mother's office[10] . After failing the exams at Southern Ural State University, Gorshkov affiliated himself with a group of hackers that called themselves the Expert Group of Protection Against Hackers[11]. The group consisted of cells of two or three hackers and paid a 30 percent protection fee to an unknown entity[2]. Gorshkov coordinated one of these cells, where Ivanov and another programmer called Michael were members[13].

In 2000, life was good for these two hackers. Gorshkov and Ivanov would hack into a supposedly secure network in the United States, explain to the network administrators when they had just done, and then offer to fix the problem for a price[14]. The companies paid the programmers in cash ranging from $80 to $4,000[15]. Cognizant Technology Solutions (CTS), headquartered in Seattle, Washington, even gave the hackers storage space on its servers[16].

In June 2000, Gorshkov received an email from Seattle company called Invita Security, asking him whether he would like to work for a cybersecurity company in America[17]. Gorshkov jumped at the opportunity, traveling with Ivanov for 48 hours to interview with the company[18]. At the interview, the two hackers demonstrated their hacking skills, and the two programmers logged into their computers in Chelyabinsk[19]. When the meeting was over, they were driven back to their hotel[20]. The car then stopped suddenly, the doors were opened, and several FBI officers arrested them.[21]

When Speakeasy, a Seattle-based Internet service provider, had been victimized, the FBI created Operation Flyhook, a surveillance operation to arrest and then prosecute cyber criminals[23,24]. The idea was to lure hackers to the United States by offering hackers employment at a fake cybersecurity company. Because many Russian hackers were young technologists with little income, the opportunity to work in America was irresistible[25]. Even though Gorshkov and Ivanov were making a good living in Russia scamming and extorting money from American companies, the temptation to work for a company like Amazon or Google was bait too good to pass up[26]. Gorshkov and Ivanov took the bait, hook, line, and sinker.

Vasiliy Gorshkov's Case

Gorshkov was tried and convicted of 20 counts of conspiracy, and a variety of computer crimes against the Speakeasy Network of Seattle, Washington[27].

Gorshkov's attorney, Kenneth Kanev, attempted to block the use of data from the hacker's servers in Russia[28]. After Gorshkov and Ivanov were arrested, the FBI proceeded to download 1.3 to 2.7 gigabytes of data from the hacker's servers that were located in Russia[29,30]. A warrant was issued to the FBI ten days after the download occurred[31]. While the two Russian hackers were demonstrating their talents to the FBI agents posing in Invita hiring managers, a keyboard sniffer was installed on their machines unbeknownst to Gorshkov and Ivanov, recording every keystroke[32]. Because the Russian servers were located in Chelyabinsk, Kanev argued that the FBI violated Gorshkov's Fourth Amendment rights[33]. Four years later, the Supreme Court opined that no search warrant was necessary when American law enforcement a non-U.S. citizen's residence in a foreign country[34]. Gorshkov was sentenced to three years in prison and ordered to pay $692,000 in restitution[35].

Alexey Ivanov's Case

Ivanov was indicted in Connecticut for charges of conspiracy, computer fraud, extortion, and possession of illegal access devices under the Computer Fraud and Abuse Act (CFAA)[36,37]. Had Ivanov been convicted on all counts, he could have spent up to 90 years in prison[38]. After the indictment was handed down by the court, Ivanov filed a motion to dismiss all charges because he was physically located in Russia, not the United States when the offenses occurred, and thus he could not be charged with violating United States law. The federal district court denied Ivanov's motion because the harm resulting from Ivanov's action occurred in the United States and because the statutes under which he was charged were intended by Congress to apply extraterritorially. The court cited *Muench* which opined that when the intent is to cause harm inside the United States by individuals outside this country, the United States Law can be successfully applied against these individuals[39]. The court also cited *Steinberg*, where it concluded that there is ample precedent that a person could be charged where the harm occurs even if the individual was not physically present in the jurisdiction where the harm took place[40]. The court noted that the computers were located in Vernon, Connecticut where the illegal access occurred, and that there is legislative evidence indicating that the statues under which Ivanov was indicted were meant to apply .extraterritorially. At trial, Ivanov was sentenced to three years and eight months in prison and required to pay $800,000 in restitution[41].

At a later date, Ivanov pleaded guilty to several of the charges and was sentenced to four years in prison followed by three months of supervised release. Ivanov was prosecuted and convicted in California[42], New Jersey[43], and Washington[44] for similar crimes. In total, Ivanov was tried in five federal district courts for computer crime.

One event that deserves to be mentioned is that the FBI agent who was responsible for Operation Flyhook, Michael Schuler, was charged unauthorized access to computer information by Russia's FSB[45]. The purpose of the Russian complaint was to assert Russian sovereignty[46]. If the long-arm of American law can reach into another country, entice foreign nationals to come to the United States, and then arrest and prosecute them, it is apparent that the Russian Federation felt no restraint in doing the same to an American citizen[47]. In Gorshkov's trial, the federal district court ruled that Russian law does not apply to American agents[48].

What Were the Legal, National, and International Implications of the Crimes Committed by Gorshkov and Ivanov?

The issue with the outcome of these two cases is that in the future other countries will feel no compunction to searching servers located in America[49]. The United States courts have opined that America law has personal jurisdiction extraterritorially[50]. In contrast, the federal district has opined that Russian law, and probably the laws of any other nation, does not apply to American agents[51]. This result is the most likely an outgrowth of American exceptionalism, where the United States can do what it wants, where it wants, when it wants, to whomever it wants, and however it wants[52]. The issue

with the ideology is that the United States is unique among nations in that it presumes that America has a right to exist and that no other nation can question its actions[53].

The alleged Russian hack of the servers of the Democratic National Committee (DNC) can be viewed as a negative response to American exceptionalism, where the United States holds other countries to standards that it rejects for itself[54]. It should be remembered that in Special Prosecutor Robert Mueller's indictment of 12 Russians, each one of the Russians was specifically named, the address of where the hack occurred in St. Petersburg was specified, and a declaration of their rank in the Russian military was stated[55]. The question that begs to be asked is: How did Muller's team find out this information? It is more than probable that the Russian military computers were hacked in violation of Russian law[56]. It serves as a striking example of American exceptionalism, where the rule is: Do as I say, not as I do.

What Was the Impact of the Crimes Committed by Gorshkov and Ivanov?

According to Lemos, the cases against Gorshkov and Ivanov were extremely dangerous because they open Pandora's box where in the future, individuals as well as corporations could be criminally charged for conducting corporate espionage, particularly if the entities are headquartered in different countries[57]. In many cases, the CFAA exempts law enforcementofficers from being prosecuted if they engage in an unauthorized entry into a computer[58]. Unauthorized entry can be compared to an FBI officer driving a car beyond the speed limit to in pursuit of a criminal. Any evidence obtained when law enforcement breaks the law in performance of their duties is admissible in court[59].

When evidence is obtained from a foreign country, diplomatic channels are used with all of its niceties[60]. The issue with employing formal communications with other nations is the length of time it takes to receive the desired evidence, sometimes as long as six months[61]. In the Gorshkov and Ivanov cases, a six month wait would have been too long. According to the court papers, the password to one Ivanov's accounts was changed six days after the two Russians were arrested[62]. The issue with asking a foreign country to help the United States in convicting a cyber criminal located in another country is that it takes weeks and more likely months for the other nation to collect the requisite evidence[63]. Simply stated, such efforts take too much time because the United States is waiting for the evidence, it can be permanently deleted, thereby thwarting the prosecution of cybercriminals.

Conclusions

When Gorshkov and Ivanov were arrested, they were young adults in their twenties who were living in a country with few rules and regulations[64]. They were technologists who were intensely curious about computing[65]. They were not two evil Russian villains as characterized by the American mainstream media[66]. They saw themselves as entrepreneurs attempting to make their fortune in the rough and tumble world of Eastern Russia[67]. Should they have been prosecuted in the United States? According to American law, the answer is yes. What is interesting to note is that Gorshkov went back to Russia, while Ivanov stayed in the United States and is now working in New England and living more or less the American Dream[68]. It could only happen in America!

Miscellaneous Considerations

Author Contributions

The author has read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Conflicts of Interest

The author declares no conflict of interest.

Acknowledgments

Not applicable.

The following abbreviations are used in this manuscript

Abbreviations

CFAA-Computer Fraud and Abuse Act

DNC-Democratic National Committee

FBI-Federal Bureau of Investigation

FSB-Russian Federal Security Service

References

1. B. Valeriano, & R. C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press 2015).
2. Donald L. Buresh, *A Critical Evaluation of the Estonian Cyber Incident*. 1 J. of Adv, Forensic Sci. 2. 7, (November 03, 2020), DOI 10.14302/issn.2692-5915.jafs-20-3601.
3. Valeriano & Maness, *supra*, note 1.
4. *United States v. Netkysho, et al.*, 1:18-cr-00215 (D. Ct. D.C. 2018, July 13), https://www.courtlistener.com/docket/7431538/united-states-v-netyksho/.
5. Raymond Pompon, *Russian Hackers, Face to Face*, F5 Labs, (June 21, 2017), https://www.f5.com/labs/articles/threat-intelligence/russian-hackers-face-to-face.
6. Dept. of Justice Staff, *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts*, United States Department of Justice, (March 15, 2017), https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
7. *United States v. Panin*, Ct. Doc. No. 1:11-CR-0557-AT-AJB (N. D. Geo. 2016), https://www.courtlistener.com/docket/4242291/united-states-v-panin/.\
8. Art Jahnke, *Alexey Ivanov and Vasily Gorshkov: Russian Hacker Roulette*, CSO Online, (January 01, 2005), https://www.csoonline.com/article/2118241/malware-cybercrime/alexey-ivanov-and-vasiliy-gorshkov--russian-hacker-roulette.html.
9. Ariana Eunjung Cha, *Internet Dreams Turn to Crime*, The Washington Post, (May 18, 2003), https://www.washingtonpost.com/archive/politics/2003/05/18/internet-dreams-turn-to-crime/f1db56a7-513f-4c0e-8f50-541b47ad88bc/?utm_term=.dd5306d3fc07.\
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. Jahnke, supra, note \8.
15. *Id.*
16. *Id.*
17. Susan W. Brenner, & Joseph J. Schwerha IV, *Cybercrime Havens: Challenges and Solutions*, American Bar Association, (December 2007), https://heinonline.org/HOL/LandingPage?handle=hein.journals/busiltom17&div=31&id=&page=.
18. Jahnke, *supra*, note 8.
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. Pompon, supra, note 1.
24. *Id.*
25. *Id.*
26. Jahnke, *supra*, note 8.
27. John Leyden, *Russians Accuse FBI Agent of Hacking*, The Register, (August 16, 2002), https://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/.
28. *Id.*
29. Robert Lemos, *FBI "Hack" Raises Global Security Concerns*, Cnet, (March 28, 2002), https://

www.cnet.com/news/fbi-hack-raises-global-security-concerns/.

30. Jahnke, *supra*, note 8.
31. Philip Attfield, *United States v Gorshkov - Detailed Forensics and Case Study; Expert Witness Perspective*. IEEE, (2005), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1592518.
32. Lemos, *supra*, note 25.
33. *Id.*
34. *Id.*
35. Janke, supra, note 8.
36. *Id.*
37. 18 U.S.C. § 1030.
38. Janke, supra, note 8.
39. United States v. Muench, No. 97-2304 (11th Cir 1998), https://caselaw.findlaw.com/us-11th-circuit/1107178.html.
40. United States v. Steinberg, 62 F.2d 77 (2nd Cir. 1932), https://law.justia.com/cases/federal/appellate-courts/F2/62/77/1472534/
41. Janke, supra, note 8.
42. Monte Morin, U.S. Indicts Russian Citizen in Hacking Case, The Los Angeles Times, (June 21, 2001), https://www.latimes.com/archives/la-xpm-2001-jun-21-me-13124-story.html.
43. ABC News Staff, Russians Busted on Hacking Charges, ABC News, (January 07, 2006), https://abcnews.go.com/Technology/story?id=98625&page=1.
44. *Id.*
45. Mike Brunker, FBI Agent Charged with Hacking, NBC News, (August 15, 2002), http://www.nbcnews.com/id/3078784#.XFpG56D45mM.
46. Leyden, supra, note 23.
47. *Id.*
48. *Id.*
49. Lemos, supra, note 25.
50. United States v, Ivanov, 175 F.Supp. at 370.
51. Leyden, supra, note 23.
52. Ian Tyrrell, What, Exactly, Is 'American Exceptionalism'?, The Week, (October 21, 2016), https://theweek.com/articles/654508/what-exactly-american-exceptionalism.
53. *Id.*
54. Aaron Maté, The Elite Fixation with Russiagate, The Nation, (July 26, 2018), https://www.thenation.com/article/elite-fixation-russiagate/.
55. United States v. Netkysho, et al., supra, note 3.
56. Maté, supra, note 44.
57. Lemos, supra, note 29.
58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*
63. *Id.*
64. Cha, supra, note 5.
65. Pompon, supra, note 1.
66. *Id.*
67. *Id.*
68. Janke, supra, note 8.