UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA	:	
v.	:	Crim. No. 3:00CR00183(AWT)
ALEKSEY VLADIMIROVICH IVANOV, a/k/a ALEXEY IVANOV, a/k/a “subbsta”	:	

RULING ON MOTION TO DISMISS

Defendant Aleksey Vladimirovich Ivanov (“Ivanov”) has been indicted, in a superseding indictment, on charges of conspiracy, computer fraud and related activity, extortion and possession of unauthorized access devices. Ivanov has moved to dismiss the indictment on the grounds that the court lacks subject matter jurisdiction. Ivanov argues that because it is alleged that he was physically located in Russia when the offenses were committed, he can not be charged with violations of United States law. For the reasons set forth below, the defendant’s motion is being denied.

I. Background

Online Information Bureau, Inc. (“OIB”), the alleged victim in this case, is a Connecticut corporation based in Vernon, Connecticut. It is an “e-commerce” business which assists retail and Internet merchants by, among other things, hosting their websites and processing their credit card data

and other financial transactions. In this capacity, OIB acts as a financial transaction "clearinghouse", by aggregating and assisting in the debiting or crediting of funds against each account for thousands of retail and Internet purchasers and vendors. In doing so, OIB collects and maintains customer credit card information, merchant account numbers, and related financial data from credit card companies and other financial institutions.

The government alleges that Ivanov "hacked" into OIB's computer system and obtained the key passwords to control OIB's entire network. The government contends that in late January and early February 2000, OIB received from Ivanov a series of unsolicited e-mails indicating that the defendant had obtained the "root" passwords for certain computer systems operated by OIB. A "root" password grants its user access to and control over an entire computer system, including the ability to manipulate, extract, and delete any and all data. Such passwords are generally reserved for use by the system administrator only.

The government claims that Ivanov then threatened OIB with the destruction of its computer systems (including its merchant account database) and demanded approximately $10,000 for his assistance in making those systems secure. It claims, for example, that on February 3, 2000, after his initial solicitations had been rebuffed, Ivanov sent the following e-

mail to an employee of OIB:

> [name redacted], now imagine please Somebody hack you network (and not notify you about this), he download Atomic software with more than 300 merchants, transfer money, and after this did 'rm-rf/' and after this you company be ruined. I don't want this, and because this i notify you about possible hack in you network, if you want you can hire me and im allways be check security in you network. What you think about this?[1]

The government contends that Ivanov's extortionate communications originated from an e-mail account at Lightrealm.com, an Internet Service Provider based in Kirkland, Washington. It contends that while he was in Russia, Ivanov gained access to the Lightrealm computer network and that he used that system to communicate with OIB, also while he was in Russia. Thus, each e-mail sent by Ivanov was allegedly transmitted from a Lightrealm.com computer in Kirkland, Washington through the Internet to an OIB computer in Vernon, Connecticut, where the e-mail was opened by an OIB employee.[2]

---

[1] An individual with "root access" who inputs the UNIX command "rm-rf/" will delete all files on the network server, including all operating system software.

[2] Originally based on signal transmissions over telephone lines, the Internet connects computers and their users by means of a universal protocol, known as the Internet Protocol, or IP. The Internet assigns a unique IP address to each computer on the Internet and uses those addresses to relay "packets", i.e. small chunks of digital correspondence. "When you send information across the Internet, the Transmission Control Protocol (TCP) first breaks it up into packets. Your computer sends those packets to your local network, Internet Service Provider (ISP), or online service. From there, the packets travel through many levels of networks, computers, and communications lines before they reach their final destination, which might be across town or around the world. A variety of

The parties agree that the defendant was physically located in Russia (or one of the other former Soviet Bloc countries) when, it is alleged, he committed the offenses set forth in the superseding indictment.

The superseding indictment comprises eight counts. Count One charges that beginning in or about December 1999, or earlier, the defendant and others conspired to commit the substantive offenses charged in Counts Two through Eight of the indictment, in violation of 18 U.S.C. § 371. Count Two charges that the defendant, knowingly and with intent to defraud, accessed protected computers owned by OIB and by means of this conduct furthered a fraud and obtained something of value, in violation of 18 U.S.C. §§ 2, 1030(a)(4) and 1030(c)(3)(A). Count Three charges that the defendant intentionally accessed protected computers owned by OIB and thereby obtained information, which conduct involved interstate and foreign communications and was engaged in for purposes of financial gain and in furtherance of a criminal act, in violation of 18 U.S.C. §§ 2, 1030(a)(2)(C) and 1030(c)(2)(B). Counts Four and

---

hardware processes those packets and routes them to their proper destinations." Preston Gralla, How the Internet Works 9 (1999). The target computer then compiles the incoming packets and executes its processes accordingly. For example, an incoming packet might request the target computer to relay back images and text to be displayed as a web page on the requestor's Internet browser, or a series of incoming packets might be assembled as an email to be delivered to a user on the target's computer system. Id.

Five do not pertain to this defendant.

Count Six charges that the defendant transmitted in interstate and foreign commerce communications containing a threat to cause damage to protected computers owned by OIB, in violation of 18 U.S.C. §§ 1030(a)(7) and 1030(c)(3)(A). Count Seven charges that the defendant obstructed, delayed and affected commerce, and attempted to obstruct, delay and affect commerce, by means of extortion by attempting to obtain property from OIB with OIB's consent, inducing such consent by means of threats to damage OIB and its business unless OIB paid the defendant money and hired the defendant as a security consultant, in violation of 18 U.S.C. § 1951(a). Count Eight charges that the defendant, knowingly and with intent to defraud, possessed unauthorized access devices, which conduct affected interstate and foreign commerce, in violation of 18 U.S.C. §§ 1029(a)(3).

II. Discussion

The defendant and the government agree that when Ivanov allegedly engaged in the conduct charged in the superseding indictment, he was physically present in Russia and using a computer there at all relevant times. Ivanov contends that for this reason, charging him under the Hobbs Act, 18 U.S.C. § 1951, under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and under the access device statute, 18 U.S.C. § 1029,

would in each case require extraterritorial application of that law and such application is impermissible. The court concludes that it has jurisdiction, first, because the intended and actual detrimental effects of Ivanov's actions in Russia occurred within the United States, and second, because each of the statutes under which Ivanov was charged with a substantive offense was intended by Congress to apply extraterritorially.

A. The Intended and Actual Detrimental Effects of the Charged Offenses Occurred Within the United States

As noted by the court in United States v. Muench, 694 F.2d 28 (2d Cir. 1982), "[t]he intent to cause effects within the United States . . . makes it reasonable to apply to persons outside United States territory a statute which is not expressly extraterritorial in scope." Id. at 33. "It has long been a commonplace of criminal liability that a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit." United States v. Steinberg, 62 F.2d 77, 78 (2d Cir. 1932). "[T]he Government may punish a defendant in the same manner as if [he] were present in the jurisdiction when the detrimental effects occurred." Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 666 (2d Cir. 1983).

The Supreme Court has quoted with approval the following language from Moore's International Law Digest:

The principle that a man, who outside of a country

> willfully puts in motion a force to take effect in it, is answerable at the place where the evil is done, is recognized in the criminal jurisprudence of all countries. And the methods which modern invention has furnished for the performance of criminal acts in that manner has made this principle one of constantly growing importance and of increasing frequency of application.

Ford v. United States, 273 U.S. 593, 623 (1927). Moreover, the court noted in Rich that:

> [I]t is certain that the courts of many countries, even of countries which have given their criminal legislation a strictly territorial character, interpret criminal law in the sense that offences, the authors of which at the moment of commission are in the territory of another State, are nevertheless to be regarded as having been committed in the national territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there. The S. S. Lotus, 1927 P.C.I.J., ser. A, No. 10, at 23, reprinted in 2 Hudson, World Court Reports, 23, 38 (1935).

Rich, 707 F.2d at 666.

Here, all of the intended and actual detrimental effects of the substantive offenses Ivanov is charged with in the indictment occurred within the United States. In Counts Two and Three, the defendant is charged with accessing OIB's computers. Those computers were located in Vernon, Connecticut. The fact that the computers were accessed by means of a complex process initiated and controlled from a remote location does not alter the fact that the accessing of the computers, i.e. part of the detrimental effect prohibited by the statute, occurred at the place where the computers were physically located, namely OIB's place of business in Vernon,

Connecticut.

Count Two charges further that Ivanov obtained something of value when he accessed OIB's computers, that "something of value" being the data obtained from OIB's computers. In order for Ivanov to violate § 1030(a)(4), it was necessary that he do more than merely access OIB's computers and view the data. See United States v. Czubinski, 106 F.3d 1069, 1078 (6th Cir. 1997) ("[M]erely viewing information cannot be deemed the same as obtaining something of value for purposes of this statute." . . . [T]his section should apply to those who steal information through unauthorized access . . . ."). The indictment charges that Ivanov did more than merely gain unauthorized access and view the data. Ivanov allegedly obtained root access to the OIB computers located in Vernon, Connecticut. Once Ivanov had root access to the computers, he was able to control the data, e.g., credit card numbers and merchant account numbers, stored in the OIB computers; Ivanov could copy, sell, transfer, alter, or destroy that data. That data is intangible property of OIB. See Carpenter v. United States, 484 U.S. 19, 25 (1987) (noting that the "intangible nature [of confidential business information] does not make it any less 'property' protected by the mail and wire fraud statutes."). "In determining where, in the case of intangibles, possession resides, the measure of control exercised is the deciding factor." New York Credit Men's Ass'n v. Mfrs. Disc. Corp., 147 F.2d 885, 887 (2d Cir.

1945).

At the point Ivanov gained root access to OIB's computers, he had complete control over that data, and consequently, had possession of it. That data was in OIB's computers. Since Ivanov possessed that data while it was in OIB's computers in Vernon, Connecticut, the court concludes that he obtained it, for purposes of § 1030(a)(4), in Vernon, Connecticut. The fact that Ivanov is charged with obtaining OIB's valuable data by means of a complex process initiated and controlled from a remote location, and that he subsequently moved that data to a computer located in Russia, does not alter the fact that at the point when Ivanov first possessed that data, it was on OIB's computers in Vernon, Connecticut.

Count Three charges further that when he accessed OIB's computers, Ivanov obtained information from protected computers. The analysis as to the location at which Ivanov obtained the information referenced in this count is the same as the analysis as to the location at which he obtained the "something of value" referenced in Count Two. Thus, as to both Counts Two and Three, it is charged that the balance of the detrimental effect prohibited by the pertinent statute, i.e., Ivanov's obtaining something of value or obtaining information, also occurred within the United States.

Count Six charges that Ivanov transmitted a threat to cause damage to protected computers. The detrimental effect

prohibited by § 1030(a)(7), namely the receipt by an individual or entity of a threat to cause damage to a protected computer, occurred in Vernon, Connecticut because that is where OIB was located, where it received the threat, and where the protected computers were located. The analysis is the same as to Count Seven, the charge under the Hobbs Act.

Count Eight charges that Ivanov knowingly and with intent to defraud possessed over ten thousand unauthorized access devices, i.e., credit card numbers and merchant account numbers. For the reasons discussed above, although it is charged that Ivanov later transferred this intangible property to Russia, he first possessed it while it was on OIB's computers in Vernon, Connecticut. Had he not possessed it here, he would not have been able to transfer it to his computer in Russia. Thus, the detrimental effect prohibited by the statute occurred within the United States.

Finally, Count One charges that Ivanov and others conspired to commit each of the substantive offenses charged in the indictment. The Second Circuit has stated that "the jurisdictional element should be viewed for purposes of the conspiracy count exactly as we view it for purposes of the substantive offense . . . ." United States v. Blackmon, 839 F.2d 900, 910 (2d Cir. 1988) (internal citations and quotation marks omitted). See also United States v. Kim, 246 F.3d 186, 191, n.2 (2d Cir. 2001) (noting that jurisdiction over a

conspiracy charge depends upon jurisdiction over the underlying substantive charge). Federal jurisdiction over a conspiracy charge "is established by proof that the accused planned to commit a substantive offense which, if attainable, would have violated a federal statute, and that at least one overt act has been committed in furtherance of the conspiracy." United States v. Giordano, 693 F.2d 245, 249 (2d Cir. 1982). Here, Ivanov is charged with planning to commit substantive offenses in violation of federal statutes, and it is charged that at least one overt act was committed in furtherance of the conspiracy. As discussed above, the court has jurisdiction over the underlying substantive charges. Therefore, the court has jurisdiction over the conspiracy charge, at a minimum, to the extent it relates to Counts Two, Three, Six, Seven or Eight.

Accordingly, the court concludes that it has subject matter jurisdiction over each of the charges against Ivanov, whether or not the statutes under which the substantive offenses are charged are intended by Congress to apply extraterritorially, because the intended and actual detrimental effects of the substantive offenses Ivanov is charged with in the indictment occurred within the United States.

B. Intended Extraterritorial Application

The defendant's motion should also be denied because, as

to each of the statutes under which the defendant has been indicted for a substantive offense, there is clear evidence that the statute was intended by Congress to apply extraterritorially. This fact is evidenced by both the plain language and the legislative history of each of these statutes.

There is a presumption that Congress intends its acts to apply only within the United States, and not extraterritorially. However, this "presumption against extraterritoriality" may be overcome by showing "clear evidence of congressional intent to apply a statute beyond our borders . . . ." U.S. v. Gatlin, 216 F.3d 207, 211 (2d Cir. 2000). "Congress has the authority to enforce its laws beyond the territorial boundaries of the United States. Whether Congress has in fact exercised that authority in [a particular case] is a matter of statutory construction." Equal Employment Opportunity Comm. v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) (internal citations omitted) ("ArAmCo").

The defendant is charged with substantive offenses in violation of 18 U.S.C. § 1951, 18 U.S.C. § 1030 and 18 U.S.C. § 1029, and with conspiracy in violation of 18 U.S.C. § 371.

1. 18 U.S.C. § 1951: The Hobbs Act

The Hobbs Act provides, in pertinent part, as follows:

> Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens

> physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both.

18 U.S.C. § 1951(a) (West 2000).

The Supreme Court has stated that the Hobbs Act "speaks in broad language, manifesting a purpose to use all the constitutional power Congress has to punish interference with interstate commerce by extortion, robbery or physical violence." Stirone v. United States, 361 U.S. 212, 215 (1960). The Court has not had occasion to decide whether the "broad language" of the Hobbs Act expresses a congressional intent to apply the statute extraterritorially. However, the Third Circuit, relying in part on Stirone, concluded that:

> [E]ven if none of the [defendants'] overt acts had occurred in this country . . . Congress could give the district court jurisdiction under the commerce clause so long as [the defendants'] activities affected [the victim's] commercial ventures in interstate commerce within the United States. See Stirone v. United States, 361 U.S. 212, 215, 80 S.Ct. 270, 272, 4 L.Ed.2d 252 (1960) (Hobbs Act utilizes all of Congress's commerce clause power and reaches even a minimal interference with commerce) . . . ."

United States v. Inigo, 925 F.2d 641, 648 (3d Cir. 1991).

Based on the foregoing, this court concludes that the Hobbs Act encompasses not only all extortionate interference with interstate commerce by means of conduct occurring within the United States, but also all such conduct which, although it occurs outside the United States, affects commerce within the

borders of the United States. Therefore, it is immaterial whether Ivanov's alleged conduct can be said to have taken place entirely outside the United States, because that conduct clearly constituted "interference with interstate commerce by extortion", Stirone, 361 U.S. at 215, in violation of the Hobbs Act. Consequently, the court has jurisdiction over this charge against him.

2. 18 U.S.C. § 1030: The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") was amended in 1996 by Pub. L. No. 104-294, 110 Stat. 3491, 3508. The 1996 amendments made several changes that are relevant to the issue of extraterritoriality, including a change in the definition of "protected computer" so that it included any computer "which is used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B) (emphasis added). The 1996 amendments also added subsections (a)(2)(C) and (a)(7), which explicitly address "interstate or foreign commerce", and subsection (e)(9), which added to the definition of "government entity" the clause "any foreign country, and any state, province, municipality or other political subdivision of a foreign country".[3]

The plain language of the statute, as amended, is clear.

[3] This change extends to foreign governments the protections of subsection (a)(7) against computer extortion.

Congress intended the CFAA to apply to computers used "in interstate or foreign commerce or communication." The defendant argues that this language is ambiguous. The court disagrees. The Supreme Court has often stated that "a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." Regions Hosp. v. Shalala, 522 U.S. 448, 467 (1998)(internal citations and quotation marks omitted). In order for the word "foreign" to have meaning, and not be superfluous, it must mean something other than "interstate". In other words, "foreign" in this context must mean international. Thus, Congress has clearly manifested its intent to apply § 1030 to computers used either in interstate or in foreign commerce.

The legislative history of the CFAA supports this reading of the plain language of the statute. The Senate Judiciary Committee issued a report explaining its reasons for adopting the 1996 amendments. S. Rep. No. 357, 104th Congr., 2d Sess. (1996). In that report, the Committee specifically noted its concern that the statute as it existed prior to the 1996 amendments did not cover "computers used in foreign communications or commerce, despite the fact that hackers are often foreign-based." Id. at 4. The Committee cited two specific cases in which foreign-based hackers had infiltrated computer systems in the United States, as examples of the kind

of situation the amendments were intended to address:

> For example, the 1994 intrusion into the Rome Laboratory at Grifess Air Force Base in New York, was perpetrated by a 16-year-old hacker in the United Kingdom. More recently, in March 1996, the Justice Department tracked down a young Argentinean man who had broken into Harvard University's computers from Buenos Aires and used those computers as a staging ground to hack into many other computer sites, including the Defense Department and NASA.

Id. at 4-5. Congress has the power to apply its statutes extraterritorially, and in the case of 18 U.S.C. § 1030, it has clearly manifested its intention to do so.

3. 18 U.S.C. § 1029: The Access Device Statute

Section 1029 of Title 18 of the United States Code provides for the imposition of criminal sanctions on any person who uses, possesses or traffics in a counterfeit access device "if the offense affects interstate or foreign commerce." 18 U.S.C. § 1029 (2000). As noted above, there is a centuries old canon of statutory construction to the effect that a statute should be construed so that no word or phrase is rendered superfluous. See, e.g., Platt v. Union Pac. R.R. Co., 99 U.S. 48, 58 (1878)(noting that the "rules of statutory construction declare that a legislature is presumed to have used no superfluous words."). Therefore, based on the same reasoning applied above in the discussion of § 1030, the court concludes that the plain language of § 1029 indicates a congressional intent to apply the statute extraterritorially.

The parties agreed at oral argument that the legislative history of 18 U.S.C. § 1029 mirrors that of § 1030. Therefore, the discussion above of the congressional intent behind § 1030 also applies to § 1029. Accordingly, the court finds that this section, too, was intended to apply extraterritorially.

4. 18 U.S.C. § 371: The Conspiracy Statute

The Second Circuit has recently noted that where the court has jurisdiction over the underlying substantive criminal counts against a defendant, the court also has jurisdiction over the conspiracy counts. See Kim, 246 F.3d at 191, n.2. A court may "infer[] the extra-territorial reach of conspiracy statutes on the basis of a finding that the underlying substantive statute reached extra-territorial offenses, even though the conspiracy charges came under separate code sections . . . ." United States v. Evans, 667 F. Supp. 974, 981 (S.D.N.Y. 1987) (internal quotation marks and citations omitted). See also United States v. Yousef, 927 F. Supp. 673, 682 (S.D.N.Y. 1996) ("Extraterritorial jurisdiction over a conspiracy charge depends on whether extraterritorial jurisdiction exists as to the underlying substantive crime.") Because the court finds that each of the underlying substantive statutes in this case was intended by Congress to apply extraterritorially, it also finds that it has jurisdiction over the conspiracy charge.

IV. Conclusion

For the reasons set forth above, the defendant's Motion to Dismiss for Lack of Subject Matter Jurisdiction [Doc. # 34] is hereby DENIED.

It is so ordered.

Dated this 6th day of December, 2001 at Hartford, Connecticut.

Alvin W. Thompson
United States District Judge