Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

"Hacktivists" and the Ukraine-Russia Conflict: Legal Considerations

Jonathan M. Gaffney
Legislative Attorney

May 13, 2022

Since Russia's February 24, 2022, invasion of Ukraine, a growing number of nongovernmental hackers motivated by social or political objectives—so-called "hacktivists"—have conducted offensive cyberspace operations against Russia. Some of these groups and individuals may be responding to a February 26 tweet by Mykhailo Fedorov, Ukraine's Vice Prime Minister and Minister of Digital Transformation, who called for the creation of a volunteer "IT Army." One scholar has cited this invitation as "the first time that states have openly called for citizens and volunteers to cyberattack another state."

Ukraine's volunteer IT Army—which may include "hundreds of thousands of hackers" from within and outside Ukraine—may be working on "operational tasks" identified by the Ukrainian government. This volunteer organization joins the International Legion of Ukraine as a way for foreign volunteers to participate in the conflict. However, just as participation in the International Legion might result in adverse legal consequences for volunteers who are U.S. nationals, various federal statutes might be implicated should U.S. persons join the IT Army or otherwise conduct cyberspace operations against Russian assets.

This Sidebar considers potential civil and criminal liability under federal law for individuals within the United States who hack foreign governmental or nongovernmental computers. It first discusses the potential applicability of two federal statutes to alleged hostile or malicious cyber activities targeting Russia by hacktivists residing in the United States: the Computer Fraud and Abuse Act (CFAA) and the Neutrality Act. It then presents several considerations for Congress as this situation evolves. Although this Sidebar generally discusses volunteers acting on Ukraine's behalf, the analysis below would also likely apply to U.S. persons acting on Russia's behalf against Ukraine.

Congressional Research Service
7-5700
www.crs.gov
LSB10743

The CFAA

One law potentially applicable to U.S. individuals who hack foreign computers is the CFAA, which prohibits a variety of computer-related conduct and imposes civil and criminal penalties for violations of its provisions. As potentially relevant to U.S.-based hackers targeting foreign computers, the CFAA prohibits, among other things,

- intentionally accessing a computer without authorization or in excess of authorization and obtaining certain information from a financial institution or a protected computer (18 U.S.C. 1030(a)(2)(A)-(C));
- knowingly accessing a protected computer without authorization or in excess of authorization with the intent to defraud, if "such conduct furthers the intended fraud and [the violator] obtains anything of value" (18 U.S.C. § 1030(a)(4));
- intentionally damaging a protected computer by knowingly transmitting a program, information, code, or command (18 U.S.C. § 1030(a)(5));
- knowingly, and with intent to defraud, trafficking in passwords or similar information granting access to a computer where such trafficking affects foreign commerce (18 U.S.C. § 1030(a)(6)); and
- threatening to cause damage or obtain information from protected computers with an intent to extort money or another thing of value (18 U.S.C. § 1030(a)(7)).

For purposes of the CFAA, a *computer* is any "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions," including "any data storage facility or communications facility directly related to or operating in conjunction with such device . . . ." Courts have interpreted this definition broadly to include "any device that makes use of a[n] electronic data processor," including personal computers, servers, cell phones, smart devices, and infrastructure controllers.

The CFAA defines a *protected computer* as, among other things, computers "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." As with the CFAA's definition of *computer*, courts have construed the meaning of *protected computer* broadly to include "effectively any computer connected to the Internet." In addition, at least one court has explained that the CFAA applies to acts committed by individuals in the United States against protected computers outside the United States, as unauthorized conduct "basically happens simultaneously at the locations of the accessor and the accessed computer." For more information about the CFAA, see CRS Report R46536, *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*, by Peter G. Berris.

The CFAA and the Ukraine-Russia Conflict

Given the expansive definitions of *computer* and *protected computer*, it appears that the CFAA could apply to individuals in the United States who engage in prohibited activities with respect to foreign computer systems outside the United States. This liability could conceivably arise in several ways. For example, news reports indicate that Ukraine-backed hackers have planned attacks on Russian railways and its electrical grid. To the extent that these elements of Russia's infrastructure meet the CFAA's definition of *protected computer*, provisions such as § 1030(a)(5)(A)—prohibiting intentional damage of a protected computer through the knowing transmission of a program, code, or command—could potentially apply to attacks on Russian computers in the same way such attacks taking place entirely within the United States would be subject to this provision. This could occur, for example, if a hacker

located in the United States (whether or not a U.S. citizen or national) knowingly transmitted a virus with the intent of damaging Russian infrastructure, causing it to malfunction. Similarly, ransomware attacks against Russian systems could potentially violate § 1030(a)(7), the CFAA's prohibitions on damaging protected computers or threatening to do so with intent to commit extortion.

Although the CFAA might apply as a matter of law to U.S. hackers' attacks on Russian computers, it is unclear, as a practical matter, whether the U.S. Department of Justice would choose to prosecute such conduct. It also seems doubtful that Russia would cooperate with prosecutors or even reveal whether such cyberattacks had occurred, particularly in light of reports that it is trying to downplay and censor its casualty numbers.

The Neutrality Act

Since 1794, the Neutrality Act and its precursors have prohibited U.S. nationals from taking certain actions "against the territory or dominion of any foreign prince or state, or of any colony, district, or people with whom the United States is at peace." Among other conduct, the Neutrality Act prohibits U.S. nationals from accepting a military commission or enlisting in a foreign military while within the jurisdiction of the United States, with limited exceptions.

One provision of the Neutrality Act—18 U.S.C. § 960—prohibits individuals, while on U.S. soil, from beginning, preparing the means for, furnishing the money for, or taking part in "any military or naval expedition or enterprise" against a nation with whom the United States is at peace. While this section seems to potentially encompass U.S. hackers targeting foreign computers, particularly if doing so would aid another country engaged in hostilities with the target, it does not appear that § 960 has ever been applied to individuals engaged in hacking or other cyber activities. On the contrary, more than a century ago in *Wiborg v. United States*, the Supreme Court defined *military expedition* narrowly as "a journey or voyage by a company or body of persons, having the position or character of soldiers, for a specific warlike purpose." The Court has not considered the scope of § 960 since 1896, and it is possible that a court could revisit this issue. Several legal scholars have recognized this possibility, citing the growing rise of cyber warfare and an evolving understanding of the types of conduct that constitute military action to speculate that § 960 could potentially be applied to hacking or other cyberattacks. Under the current definition of *military expedition or enterprise*, however, it seems unlikely that U.S. hackers could violate § 960 through purely cyber activities. One possible exception might be if the hackers' activities "provide[d] or prepare[d] a means for" a military expedition or enterprise, such as gathering intelligence about Russian troop positions that was used by Ukraine to launch a conventional attack. For more information about the Neutrality Act, see CRS In Focus IF12068, *U.S. Nationals and Foreign Military Service*, by Jennifer K. Elsea, Jonathan M. Gaffney, and Alan Ott.

Considerations for Congress

It appears that U.S. hackers' involvement in the Ukraine-Russia conflict could violate the CFAA and, under certain circumstances, the Neutrality Act. Those laws, however, contain enough ambiguity that it is unclear whether courts would find those laws applicable to such actions by a U.S.-based group or individual. It is also unclear whether the Department of Justice would prosecute any such offenses or whether Russia would cooperate with any investigations necessary to prosecute such conduct.

If Congress believes that current laws do not adequately prohibit U.S. hackers' participation in foreign conflicts, it may seek to clarify the scope of the CFAA or Neutrality Act to unambiguously proscribe attacks on foreign governments' computers. For example, Congress could define *military expedition* under § 960 to include offensive cyberspace operations. If Congress were to do so, § 960 would likely prohibit additional conduct, such as a foreign government's cyberattack on another nation with the

participation of U.S. volunteers, or U.S. hackers supplying a foreign government with passwords or information regarding vulnerabilities in another nation's systems. Depending on how broadly Congress statutorily defines *military expedition*, it might be possible for U.S. hackers acting independently from a foreign government to violate § 960, just as the Supreme Court has recognized that "[a] few men deluded with the belief of their ability to overturn an existing government or empire" may do so when launching a conventional military expedition.

Conversely, if Congress wanted to explicitly allow U.S. hackers' assistance to Ukraine or other foreign powers faced with unprovoked attacks, it might consider amending the CFAA and Neutrality Act to exempt cyberspace operations against foreign governments in limited circumstances. Allowing this exception, however, may have unintended domestic or foreign policy consequences, such as the target of these cyberspace operations viewing them as sanctioned by the U.S. government. There has been a great deal of debate regarding the advisability and legality of counterattacks against initial hacks—so-called "hacking back"—and it seems likely that concerns raised with respect to this topic would be exacerbated in the context of foreign relations if such provisions were adopted.

Absent congressional action, courts could potentially determine whether the CFAA or Neutrality Act apply to U.S. hackers' attacks on foreign computers. As discussed above, such judicial action could possibly include revisiting the definition of *military expedition or enterprise* under § 960 in light of an evolving understanding of that phrase. A court's ability to reach these issues, however, would depend on whether the Department of Justice prosecutes alleged violations of those acts and the degree to which a foreign government cooperates with such prosecutions.