(C., Palmer C., 2001, p. 861)

(Trabelsi et al., 2016, p. 861)

Hacking should be considered a crime if it is:

* Compromising national security
* Hacking with malicious intents

The intention of the act is what makes it a criminal act or an essential method to ensure the security of the nation.

--ddos

--Anonymous: these threats are criminal. The messages are delivered with malicious intent and they seem to compromise national security.

Look into how foreign cases were handled and how FSIA laws play a role.

*GOOD*

*BAD*

1A Hacking Competitions and Their Untapped Potential for Security Educatio

Baggs, J., Gee, J., Lewis, E., & Fowler, G. (2011, May). The vaccine safety datalink: A model for monitoring immunization safety. *Pediatrics*, 127, 45-53. doi: 10.1542/peds.2010-1722H

Conti, G., Babbitt, T. & Nelson J. (2011, May). Hacking competitions and their untapped potential for security education. *IEEE Security & Privacy*, 9(3), 56-59. doi: 10.1109/MSP.2011.51

These competitions test participants’ ingenuity and problem-solving skills, are fun and innovative, and draw large, enthusiastic groups of participants and spectators. Pg. 56

By learning the hacker perspective and considering the unanticipated use of technology, students will be better prepared to deter attacks and defend against them. Pg. 56

Wireless-networking technologies are on the rise, and wireless vulnerabilities and open access points are increasingly common. Hacker competitions highlight these concerns. For example, war-driving competitions, during which participants map open access points, quantitatively illustrate the prevalence of insecure system configurations and raise public awareness. Pg. 56-57

Competitions have spurred new antenna designs and illustrated that consumer-grade wireless-network transmissions are vulnerable at extreme distances. Pg 57

Educators can use wireless hacking events to emphasize many learning objectives, such as ethics, privacy rights, ??antenna design??, networking protocols, and the importance of usable security pg 57

DEF CON’s Crack Me if You Can hash-cracking competition challenges participants to illustrate weaknesses in the username/password paradigm by working backward from hashes to passwords.pg 57

Attacks have recently increased against end-user application software, including Web browsers, word processors, and document viewers. One long-term solution is to teach secure coding practices that eliminate many vulnerabilities early during software development, instead of dealing with them through postdiscovery patches. Pg 57

DEF CON’s Race to Zero contest challenged contestants to modify malicious code samples to bypass antivirus software, while still maintaining a functional payload.8 This contest helped determine the real-world difficulty of avoiding detection by different classes of antivirus software. Pg 58

An important component of an information security curriculum is effectively communicating technical security and privacy principles, including to a non-tech-savvy public. Pg 58

Hacking competitions can help educators infuse learning and excitement into information security education programs. Pg 59

2B Ethical Hacking in Information Security Curricula

Baggs, J., Gee, J., Lewis, E., & Fowler, G. (2011, May). The vaccine safety datalink: A model for monitoring immunization safety. *Pediatrics*, 127, 45-53. doi: 10.1542/peds.2010-1722H

Trabelsi, Z. & McCoey, M. (Jan., 2016). Ethical hacking in information security curricula. *International Journal of Information and Communication Technology*, 12(1), 1-10.

Furthermore, a learning environment that does not give the student an opportunity to experiment and practice with security technologies does not equip him/her with the skills and knowledge required for doing research and development in the computer security field. Pg 1

From each laboratory exercise students learn how to perform a specific attack, and how to prevent malicious hosts from performing it successfully. Pg 2

Second students will deepen their understanding of information security as they become aware of the technology’s weaknesses and vulnerabilities…pg 3

Finally adoption of the approach allows students to understand the hacker’s thought process. Pg 3

3C Ethical hacking by C. C. Palmer

Baggs, J., Gee, J., Lewis, E., & Fowler, G. (2011, May). The vaccine safety datalink: A model for monitoring immunization safety. *Pediatrics*, 127, 45-53. doi: 10.1542/peds.2010-1722H

C., Palmer C. (2001). ”Ethical hacking.” *IBM Systems Journal*, 40(3), 769-780. doi: 10.1147/sj.403.0769

In the case of computer security, these “tiger teams” or “ethical hackers” 3 would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems’ security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. (pg 770)

In one early ethical hack, the United States Air Force conducted a “security evaluation” of the Multics operating systems for “potential use as a two-level (secret/top secret) system.” 4 Their evaluation found that while Multics was “significantly better than other conventional systems,” it also had “... vulnerabilities in hardware security, software security, and procedural security” that could be uncovered with “a relatively low level of effort.” The authors performed their tests under a guideline of realism, so that their results would accurately represent the kinds of access that an intruder could potentially achieve. They performed tests that were simple information-gathering exercises, as well as other tests that were outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassi- fied reports that describe ethical hacking activities within the U.S. military. 5–7 pg 770

Most notable of these was the work ??by Farmer and Venema??, 8 which was originally posted to Usenet 9 in December of 1993. They discussed publicly, perhaps for the first time, 10 this idea of using the techniques of the hacker to assess the security of a system

* gather enough information about their targets to have been able to compromise security if they had chosen to do so.
* They provided several specific examples of how this information could be gathered and exploited to gain control of the target
* Shared how such an attack could be prevented.

Pg 770

Ethical hackers typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. Pg 771

Ethical hackers have to know the techniques of the criminal hackers, how their activities might be detected, and how to stop them. Pg 771

Types of testing

● Remote network. This test simulates the intruder launching an attack across the Internet. The primary defenses that must be defeated here are border firewalls, filtering routers, and Web servers. Pg777

● Remote dial-up network. This test simulates the intruder launching an attack against the client’s modem pools. The primary defenses that must be defeated here are user authentication schemes. These kinds of tests should be coordinated with the local telephone company.pg777

● Local network. This test simulates an employee or other authorized person who has a legal connection to the organization’s network. The primary defenses that must be defeated here are intranet firewalls, internal Web servers, server security measures, and e-mail systems.pg778

breaching and entering: when data scraping should be a federal computer hacking crime

In July 2015, hackers known as the Impact Team breached AshleyMadison.com and threatened to expose the private lives and extramarital affairs of over 30 million users.

Whether scraping constitutes hacking is most unclear when the breached data is not protected by a technical barrier but is clearly unintended for public use. This was the situation in the widely publicized case *United States v. Auernheimer*. [n28](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n28) In *Auernheimer*, which arose around the time that Apple first introduced the iPad, customers who wanted to send and receive data over cellular networks had to purchase a data contract from AT&T. Additionally, customers had to register their accounts with AT&T on a website that AT&T controlled. The customers were assigned a user identification (their email address) to access their accounts through AT&T's website. In order to make it easier for customers to log in to their accounts, AT&T programmed their servers to search for customers' identifiers based on the customers' unique URLs. The servers could then prepopulate the customers' login screens. Defendants Spitler and Auernheimer discovered AT&T's login configuration and wrote a scraper (what they called an "account slurper") to automatically access AT&T's website through different URLs and save all the different emails that AT&T generated in the login box. Through their scraper, Spitler and Auernheimer recorded 114,000 of AT&T's customers' email addresses. [n29](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n29) Although technically, the email addresses were publicly accessible, AT&T designed them to be practically inaccessible unless an individual visited the correct, publicly available URL. The case was dismissed on venue grounds, and so  [\*410]  the question of whether the defendants' scraper violated the CFAA remains open.

Harmful scrapers also often collect information without the consent of data hosts.

Finally, harmful scrapers might also collect personally identifiable information, which implicates privacy issues

Another example of a harmful scraper is one designed to automatically con people out of money. These types of scrapers were the subject of a recent case in which the Federal Trade Commission charged operators of Jerk.com for scraping personal information from Facebook to create profiles that labeled people as "jerk" or "not a jerk." [n61](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n61) The operators of Jerk.com then falsely told more than 73 million consumers, including children, that they could revise their online profiles by paying $ 30. [n62](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n62)

Another example is from *United States v. TomorrowNow Inc.*, where a scraper extracted confidential support materials from Oracle's restricted-access Customer Connection website in order to sway customers of Oracle's  [\*415]  PeopleSoft products away from Oracle. [n63](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n63) When scrapers are intentionally used to defraud and harm data hosts, consumers, and general Internet users, criminal liability is appropriate.

*Talk about troubles of making legislation in this area*

The court did not foreclose the possibility that hackers could be inside employees. Rather, it interpreted the phrase "without authorization" as designed to apply to *outside* hackers who have no authorized access to a computer and the phrase "exceeds authorized access" to apply to *inside* hackers "whose initial access to a computer is authorized but who access unauthorized information or files." [n90](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n90) Thus, the court's focus was on the *technical* means by which data was obtained. Insiders would be hackers only if they obtained data to which they did not have precise access, even if they had access to the broader network where such data was stored.

Intended use Theory. Under this theory, courts look at the underlying purpose of certain company policies to determine whether an employee breached or exceeded technically authorized access. The analysis is similar to the contract theory, but can be broader, as it considers how employees *used* the information they obtained even if those employees did not directly breach a written policy or contract.

One example of a case where this theory was adopted is *United States v. John*. [n104](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n104) There, the Fifth Circuit held that an employee violated the CFAA when she used data from Citigroup's internal computer system to obtain customer account information, which she then shared with a third party in order to engage in  [\*423]  fraudulent activity. [n105](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n105) The court stated that such use was not what the company intended when it granted her access. [n106](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n106)

Similarly, in *United States v. Rodriguez*, the Eleventh Circuit held that an employee of the United States Social Security Administration violated the CFAA when, in violation of the agency's broad policy against obtaining information for nonbusiness purposes, he obtained confidential personal information from the agency's computers that included: the social security numbers, birthdates, income, and home addresses of his ex-wife, ex-girlfriend, coworkers, and other acquaintances. [n107](http://0-www.lexisnexis.com.skyline.ucdenver.edu/lnacui2api/frame.do?tokenKey=rsh-20.393086.50033108995&target=results_DocumentContent&returnToKey=20_T25892438783&parent=docview&rand=1493565979091&reloadEntirePage=true" \l "n107)

Hacking immunity: computer attacks on United States territory by foreign sovereigns

Bagchi, Alaknanda. "Conflicting Nationalisms: The Voice of the Subaltern in Mahasweta Devi's Bashai Tudu." Tulsa Studies in Women's Literature, vol. 15, no. 1, 1996, pp. 41-50.

Schultze, Stephen J. (June, 2016). “Hacking immunity: Computer attacks on United States territory by foreign sovereigns.” *American Criminal Law Review*, 53(3), 861.

Hacking should be considered a crime if it were under the pretense of unethical intent. The advances in technology have created many new opportunities for the future, but also developed concern for the general safety of the public. This concern for safety revolves around the immense amount of data that is being constantly circulated through databases and servers. Access to this important, personal information is often encoded and restricted from public view. However, some individuals take on the challenge to break these encryptions and access restrictions to retrieve this information. People who are capable of performing such tasks and possess this technological literacy have been designated as hackers. The connotation of the word hacker has been perceived to be negative in some perspectives. In other perspectives, a hacker is defined as “individuals who creatively explore technology and push it in new directions” (hacking competitions and their untapped potential). Nonetheless, this term has two distinct definitions that can be used to describe different groups of people. The use of unethical hacking should be considered a criminal act. These malicious attacks are serve to threaten national security. Unauthorized access to American servers and computers aren’t accounted well for due to lack of proper legislation. However, these attacks can be countered with the use of ethical hacking. These practices employ organized thought and study that reveal the unethical hacker’s intents and actions. The use of ethical hacking should be allowed so that the acts of unethical hacking can be countered.

Introduce bads and then goods to finish off on positive note

Bads:

1. Information stealing

--at&t emails and other info

2. con people out of money

3. Authorized access and intended use

Goods:

Conclusion: The benefits of ethical hacking outweigh the threats posed by malicious unethical hackers that seek to violate the privacy and safety of anyone worldwide. Enforcing more positive outlooks to the practice of ethical hacking can prove to be extremely beneficial to national security and more generally any particular person’s personal computer.

On March 13, 2013, the Citizen Lab research center at the University of Toronto published the results of a detailed technical audit of suspicious Internet traffic and software. (7) The report presented strong evidence that repressive regimes around the world were using sophisticated hacking tools to spy on dissidents and opposition groups by attacking their computers. (8) These spyware tools were developed and sold to governments by a U.K.-based company named Gamma Group. (9) Subsequent revelations indicated that the Italian firm Hacking Team was selling similar high-end spyware tools to authoritarian governments without placing any meaningful limitations on their use. (10) In many cases, servers in the [United States](http://0-go.galegroup.com.skyline.ucdenver.edu/ps/i.do?p=ITOF&u=auraria_main&id=GALE|A481881269&v=2.1&it=r&sid=summon&authCount=1) were being used to control the spyware and to direct the information captured by these spyware tools back to the governmental customer. (11)

The access to technology has reached to a global scale. This means that threats to the U.S. can extend to numerous global possibilities. Such a threat needs to be accounted for as they may be unpredictable. One such example of this digital threat was published by the Citizen Lab research center at the University of Toronto on March 13, 2013. When the university came across suspicious internet traffic they investigated and uncovered the use of sophisticated hacking tools used to spy on other countries(). The reach of these hackers isn’t limited even with the limited technological state of their country. It was later found that some repressive regimes have bought spyware tools from a company named Gamma Group in U.K. (). This distribution of tools enables anyone to participate in the act of unethical hacking. This threat is dangerous as it develops concerns for national and global security. These digital attacks lead to uncovering information that could lead to drastic conflicts.

A tool from the Gamma Group in U.K. named FinSpy was supplied to a group in Ethiopia. For a long period of time, this group spied on the computer of a government employee(). These attacks were found to have compiled and transferred without the knowledge of this employee(). This crucial information could’ve lead to conflicts that would take years or decades of expenses to resolve. In another incident, “the Department of Justice indicted a Chinese businessman living in Canada for participating in a successful conspiracy to hack Boeing computer servers and steal military aircraft specifications” (). This data is highly classified and meant to be hidden from foreign attackers. These unethical hackers have what it takes to break into American computers and take the information they need. When some hackers in Iran were accused of hacking into American Bank websites and were announced to be arrested they didn’t show and were titled as fugitives(). The laws and actions taken to fight back against these hackers aren’t proving to be effective.

Five days after the Citizen Lab report, one of these alleged information flows abruptly stopped functioning. (12) The timing suggests that the government of Ethiopia had learned of the report and decided that using the Gamma tool-- "FinSpy"--had become too great a liability. Now that many targets knew they were being attacked and were working with Citizen Lab, continued use of the tool would serve only to provide Citizen Lab with further evidence. The particular flow of pilfered data that abruptly stopped after the report was published allegedly came from Mr. Kidane's computer. (13) The computer contained evidence that his Skype calls had been surreptitiously recorded and sent to a master server in Ethiopia, and that a great deal of other personal data had likewise been compiled and transferred without his knowledge. (14) Files found on the computer's hard drive indicated that someone operating a control server had instructed the FinSpy software to self-delete, but that this instruction failed to fully execute. (15)

Although cross-border computer attacks are a relatively new phenomenon, foreign sovereign immunity is a long-held principle of customary international law. Chief Justice Marshall explained in 1812 that when one sovereign permits another to enter its territory, the guest is exempt from arrest because of implicit consent of all nations. (19) To hold otherwise would be incompatible with the dignity of the guest sovereign's authority, which is equal to that of the host. (20) Subsequent decisions of the Supreme Court have framed this deference as a "matter of grace and comity." (21)

The Foreign Sovereign Immunities Act (FSIA) was drafted to account for foreign threats. However, this act was established before the existence of such complicated computer attacks ever existed(). The regulations listed in this act granted “immunity to foreign sovereigns from criminal persecution” (). These regulations don’t help to fight against the sophisticated hacking attacks that are being performed. When a different approach was taken to account for individual agents, those that were accused of the criminal act of hacking, never bothered to show up for their trial and serve their time(). All these actions serve no beneficial outcomes. When these criminals can just get away from prosecution, it seems pointless to even address the sated regulations since these regulations served no purpose to stop and prevent further crimes.

That does not mean, however, that a foreign sovereign can always act without consequence. The Foreign Sovereign Immunities Act ("FSIA") recognizes exceptions to immunity for certain types of acts. (22) In these cases, the FSIA enables a person or entity that is harmed by a foreign sovereign, or its officials or employees, to bring an action in U.S. courts. (23) When drafting the FSIA exceptions in 1976, Congress could not have contemplated today's sophisticated cross-border computer attacks. It did, however, frame the exceptions to sovereign immunity to cover a broad range of injuries. (24) Congress noted that the exception carved out for non-commercial tort injuries is intentionally "cast in general terms as applying to all tort actions for money damages." (25)

 In May 2014, the U.S. Department of Justice indicted five Chinese state employees for economic espionage alleged to have been conducted by hacking computers in the United States from China. (33) The individuals failed to appear and fugitive orders were entered. (34) Assistant Attorney General for National Security John Carlin asserted that "[s]tate actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag."

 In August of the same year, the Department of Justice indicted a Chinese businessman living in Canada for participating in a successful conspiracy to hack Boeing computer servers and steal military aircraft specifications. (36) The indictment names two unindicted co-conspirators located in China without stating whether they are affiliated with the Chinese government. (37) On March 24, 2016, the Department of Justice announced the unsealing of a recently filed indictment against seven Iranian hackers. (38) These hackers were accused of working on behalf of the Iranian government to attack American bank websites and the computer control systems of the Bowman Dam in Rye, New York.