University of Texas School of Law

Cybersecurity Foundations: Law, Policy, and Institutions

Prof. Bobby Chesney

(FALL 2017)

I. Course Description

This course is one of several cybersecurity courses sponsored by UT's Strauss Center for International Security and Law. The Strauss Center is a campus-wide interdisciplinary center that operates an array of education and research programs, one of which is called "Integrated Cybersecurity Studies," or ICS. ICS aspires to pioneer an interdisciplinary approach to graduate training relating to cybersecurity, one that integrates key elements of law, computer science, policy, engineering, and business administration. The goal is to create courses designed from the ground up to provide sophisticated "cross-training" for graduate students from all stripes.

This particular course is an important part of that larger cross-training effort. It is a hybrid course, blending law school and public affairs (with a dash of other elements, such as International Relations). The goal is to provide you with foundational knowledge concerning the nature, functions, laws, and issues relating to the various government and private actors associated with cybersecurity in the United States. During the first half of the course, we will focus on the defensive perspective. That is, we will proceed from the assumption that the overarching public-policy goal is to minimize unauthorized access to (or computer-based disruption of) computers.
The second half of the course turns things around to consider what we might characterize as the offensive perspective: situations in which the overarching public-policy goal is to *enable* rather than prevent some degree of unauthorized access to (or computer-based disruption of) computers. In both contexts, our general learning objectives are:

1. The players: Identify the roles and responsibilities of various public and private actors with respect to defense.
2. The architecture: Understand the laws, policies, and incentive structures regulating or impacting those actors.
3. The pros and cons: Grasp the pros and cons of the status quo in relation to these structures and institutions.
4. The path forward: Develop ideas for potential reform of these structures and institutions.

That's the general idea. Please note, though, that I provide much-more detailed learning objectives in the syllabus entries that follow, on a per-class basis.

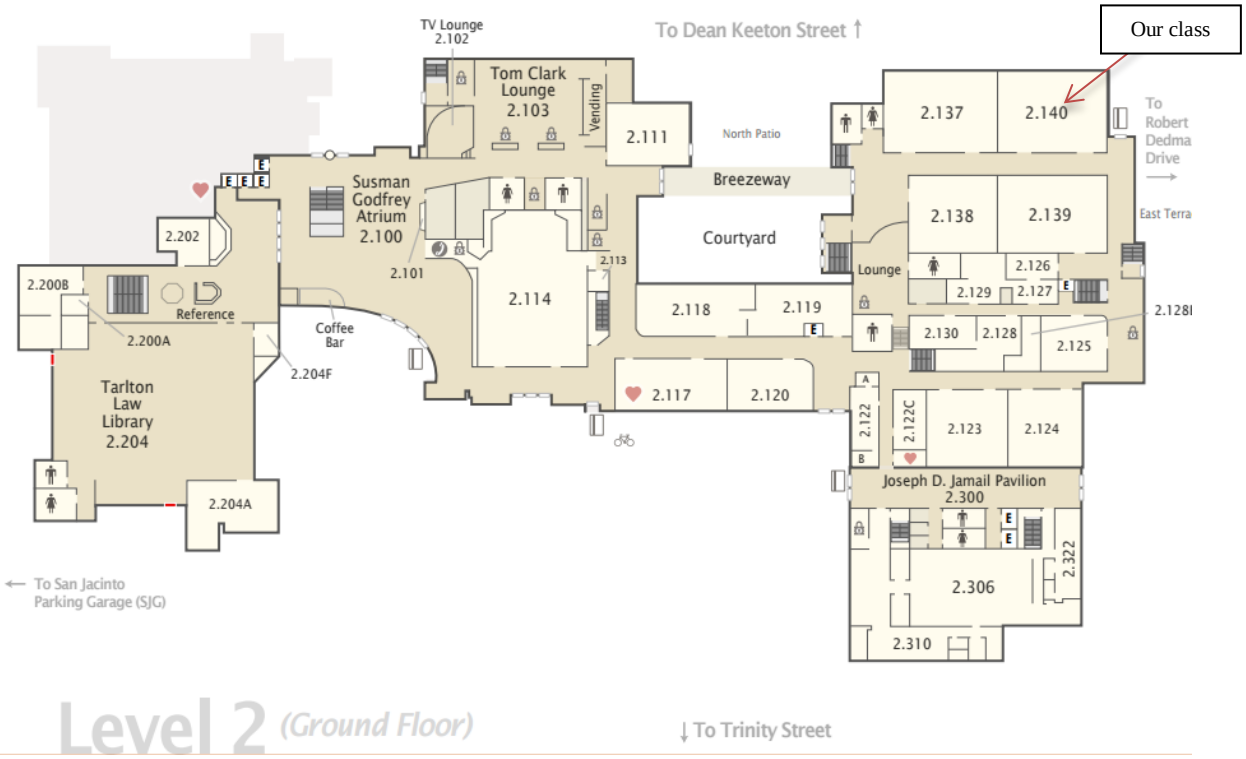
A final introductory note: I want to emphasize that this is *not* a technical course, and you do not need a technical background to understand any of it. Indeed, my assumption is that you know nothing in particular about the technologies involved. If you are a Law, Public Affairs, or Business Administration student and do want an accessible technical orientation—and you do not want to cross-register for a Computer Science or Engineering course—then I strongly recommend you also take the *other* Strauss Center "Cybersecurity Foundations" course, which is taught by Professor Tait on Monday afternoons at the Law School. It is the mirror-image of this course, focusing exclusively on tech education for non-tech students (and not touching on the law, policy, and institutional concerns that are the subject of my course). Taking both foundation courses would,

of course, be ideal for Law, Public Affairs, and Business Administration students contemplating a career in this space.

Next up: The "course policy" details, and then the syllabus.

II. COURSE POLICIES

Course id: LAW 279M (unique #29235); EE 297S (#17039); PA 280L (#60656)
First class: **Wednesday August 30th**
Schedule: Wednesday afternoons from 3:45 to 5:35
Instructor: Professor Robert Chesney (Charles I. Francis Professor in Law and Associate Dean for Academic Affairs). For more on me, see here.
Classroom: School of Law, **Townes Hall, Room 2.140** (northeast corner of the main floor)



Office hours:

Office hours are **Thursdays from 2:15 to 3:15**, or by appointment if you prefer. You are welcome to email questions anytime, too: **rchesney@law.utexas.edu**.

My office: Jones Hall 6.238 (Jones is the official name of the big concrete block building that is the western end of the law school). Elevators are in the main atrium, close to the law library's entrance. Go to the 6th floor, then use this map.

What materials will we use for the reading assignments?

All reading assignments will be posted on Canvas. You can also get free hard copies, if you prefer, from my assistant Trish Do (email her to request a copy set, at tdo@law.utexas.edu)

How much time should I expect to spend preparing for the typical class?

Expect to spend at least four to six hours in advance of each class, doing the following: (i) considering the learning objectives for that session, (ii) carefully reading the materials in light of those objectives, and (iii) pondering what you would say during class if asked to discuss any of those objectives.

How will my grade be determined?

Your grade will be a combination of two elements:

20% will be based on class participation (being there, being prepared when called upon, voluntarily joining the class conversation from time to time, participating in in-class voting exercises, and active engagement with the simulation at the end of the course), and

80% will be based on the final exam (a two-hour, open-materials test designed to reflect that which we treated as important during our class discussions; most likely the test will have a multiple-choice component as well as an essay component).

Will there be other forms of feedback aside from the final grade? More specifically, will there be any low-stakes (or no-stakes) "formative assessment" exercises?

Yes. We will use some form of online, anonymous voting in class to work our way through multiple-choice questions on an ungraded basis (though as noted above, you do have to participate).

In case I want to stay current with this topic beyond the life of this course, do you have in recommendations?

Podcasts:

Steptoe Cyberlaw Podcast - a weekly review of key legal developments relating to cybersecurity followed by in-depth interviews with a wide variety of guests

Risky Business – a weekly review of important news from the technology side of cybersecurity, also followed by in-depth interviews with a variety of guests

The National Security Law Podcast – this one normally doesn't cover much cybersecurity, but sometimes it does (and since this is the podcast co-hosted by me and Professor Vladeck, I will tout it here anyway)!

The Lawfare Podcast – again, this one normally doesn't cover cybersecurity, yet sometimes it does, so keep an eye on it as well.

Websites:

A very handy daily source of relevant news is Politico's Morning Cybersecurity:

http://www.politico.com/tipsheets/morning-cybersecurity

You would also do well to keep an eye on the two big national security law sites:

www.lawfareblog.com (which I co-founded a couple of years ago) and

www.justsecurity.org.

On-campus activities:

The Strauss Center for International Security & Law, which sponsors our course, hosts a number of speakers and events each semester, sometimes relating to cybersecurity. Sign up for our email list so you get news of events even if I forget to mention it: https://www.strausscenter.org/strauss-articles/strauss-contact.html. (Full disclosure: I am the Strauss Center Director).

The Journal on Law and Technology at Texas (JOLTT) hosts speakers, events, and other opportunities, often relating to cybersecurity. They welcome participation from a variety of students, not just law students, so reach out if you are interested!

Notice: Students with disabilities may request appropriate academic accommodations from the University's Division of Diversity and Community Engagement, Services for Students with Disabilities. Please contact the Law School Student Affairs Office with questions.

III. SYLLABUS

Below you will find a top-level overview our topics, followed by the detailed weekly assignments.

AN IMPORTANT NOTE ABOUT THE DETAILED WEEKLY ASSIGNMENTS: Each week we have a number of specific learning objectives. As you will see, I have listed them below in the form of questions you should be prepared to discuss in class. **Note that all of the supporting readings are identified *in context* with these questions (with either a link directly to the reading in question or else directions to pull the reading from our Canvas page).** This is my way of trying to ensure that you will not simply read the readings standing alone, but rather will approach them through the lens of the questions.

Top-Level Overview

I. THE DEFENSIVE PERSPECTIVE

A. Punishing Attackers

1. August 30 — Attack, Black Markets, and Crime
2. September 6 — Law Enforcement and Lawsuits
3. September 13 — Advanced Persistent Threats & State-Actor Challenges

B. Encouraging Potential Victims to Better Protect Their Systems:

4. September 20 — Mandating Better Private-Sector Defense: Regulation
5. September 27 — Motivating Better Private-Sector Defense: Litigation/Ins.
6. October 4 — Removing Barriers: Info-Sharing; Security Research
7. October 11 — Getting the Government to Protect Itself Better

C. Managing Consequences

8. October 18 — Responding to Breaches & Botnets
9. October 25 — Defense in the Context of a "Significant Cyber Incident"

II. THE OFFENSIVE PERSPECTIVE

10. November 1 — Should the Private Sector Hack Back?
11. November 8 — Law Enforcement and Network Investigative Techniques
12. November 15 — Espionage and Covert Action
13. November 29 — Armed Conflict and Cyberspace

III. CRISIS SIMULATION

14. December 6

Week-by-Week Learning Objectives and Readings

I. THE DEFENSIVE PERSPECTIVE

For the first nine weeks, we will focus on the *defensive* perspective. That is, we will focus on the overarching public-policy goals of (i) minimizing unauthorized access to (or disruption of) computers and (ii) mitigating harm when such access or disruption occurs.

When it comes to minimizing unauthorized access and disruption, the main idea is to increase both the level of difficulty attackers face and the undesirable consequences they run the risk of incurring. There is a lot of room for improvement on both accounts, currently; plenty of targets are not difficult to access or disrupt, and attackers often stand to gain much more than they realistically stand to lose. From this point of view, the goal is to have a positive, systematic impact on this balance of considerations (preferably as to all contexts, but of course progress may be more feasible in some settings than others).

At any rate, we will subdivide the defensive unit in a way that tracks these considerations. First, we will have a three-class sequence examining the current U.S. approach to impose consequences on attackers. Second, we will spend four classes examining tools that help to encourage potential victims to do more in their own defense (or, more to the point in many cases, in defense of their customers, employees, etc.). And then we will conclude with a three-class sequence regarding consequence-management when attackers nonetheless succeed.

A. Punishing Attackers

Attackers (and by that I mean no more and no less than persons or entities that seek to access a system in an unauthorized way or to disrupt the proper functioning of a system) come in many shapes and sizes. Some are sophisticated professionals, others are rank amateurs. Some are state-sponsored, some are part of non-state organized groups, and some are individuals. Some are crooks. Some are spies. Some are just showing off skills. Some are in it for the laughs. Some do it to settle personal scores, Some are seeking competitive advantage. Some just want to spur people to try harder on defense, exposing weaknesses in hopes that they'll be addressed. Some want to access your system to cause you harm, and some want to access your system so they can use it to help harm others. The point being: there are *many* potential attackers out there, with a wide variety of motives and capacities. Bear this in mind as we examine the various tools that we currently have—or might one day have—to impose consequences on attackers.

The first two classes in this three-class sequence focus on how we try to impose consequences in the most-common attack scenarios. Class 1 opens with a survey of the black markets in which stolen information, control over compromised machines, and the tools to compromise are all bought and sold. We then will introduce the Justice Department office that has primary responsibility for computer-related crimes, followed by an introduction to the Computer Fraud and Abuse Act ("CFAA"). The CFAA contains a large number of distinct criminal laws, many raising fascinating and difficult questions of interpretation and design. The CFAA also creates a "private right of action" allowing victims to sue attackers in some contexts.

In Class 2 we will dive deep into the CFAA as it has been used in practice, examining several controversial prosecutions. We also will look at other federal laws that attacks may implicate, and similar provisions found in state law and the laws of various foreign states. We also will note an international treaty that has some relevance in this setting.

In Class 3, we turn to consider a special breed of attacker: states. States sometimes attack using their own government-employed personnel, and they sometimes outsource the function to private, semi-private, and faux-private actors. At any rate, the phenomenon of state-sponsored attacks raises a host of complex questions. We will first spend some time considering concepts like attribution, deterrence, cross-domain deterrence, and escalation, and then we will look at a series of recent case studies (involving Russian and Chinese attacks on US entities) in order to understand which tools do and do not seem to have bite in this distinct setting.

(continue to the next page…)

1. August 30 – Attack, Black Markets, and Crime

The Attacker's Perspective

- Start by generating a list of reasons (stated at a high level of generality) why someone might try to gain unauthorized access to (or disrupt the functioning of) a computer or network. Bear in mind that some attackers are private individuals, while others may be part of larger organizations (private or governmental).
- When a person or entity wants to gain unauthorized access to (or disrupt the functioning of) a computer or network, it certainly helps if that person or entity has the skill and resources needed to develop tools to suit that purpose. But not everyone does, and in any event it is not necessary in all cases. There is a thriving black market for the sale not only of stolen information, but also the sale of the means to steal and disrupt. ***Read chapters 2-4 of this 2014 RAND study*** to learn more, and then consider the questions below.
- Who participates in these black markets, and has the answer to that question changed over time? Note factors such as nationality, and expertise. What are the policy implications of your answers?
- Can you explain how the types of products/services sold on the black market have changed over time as well, and why this matters from a policy perspective?
- What are botnets, and how has their use evolved over time?
- People often mention the botnet problem in connection with the growth of IoT (that is, the "Internet of Things," which is a shorthand for the growing constellation of household and personal devices with Internet connectivity of some kind). Why might that be?
- Obviously, anonymity is important to participants in the cybercrime black markets. ***Read this 2017 article*** for an introduction to how these markets and their participants try to remain hidden. Be prepared to explain what terms like "deep web," "dark web," and "TOR" signify.
- Consider which policy arguments might favor allowing at least some such hidden services to exist, and which favor suppressing them. Then consider how these interests should be balanced. Also consider whether the balance should be the same in all societies, and whether (if not) it is possible in practice to have different answers for different societies.
- Sometimes government does succeed in "taking down" a particular dark web market. The RAND report suggests such successes are "transitory," however. Why? What follows from this?
- What are "zero-day vulnerabilities" and what is special about them?

The Law Enforcement Perspective

- What is the office at DOJ that has special responsibility for this area? ***Read this.***
- What about the FBI? ***Read this for a general overview.***
- What is the role of the U.S. Secret Service, and does it make sense to have both it and the FBI involved in investigating cybercrime? ***Read this to understand USSS's role.***
- Do DOJ decision to prosecute potentially have implications—perhaps undesirable ones in some cases--for the missions of other government agencies or departments?

Introduction to the Computer Fraud and Abuse Act ("CFAA")

- There are *many* federal crimes that might be implicated by the activity we are discussing, but one that plays an especially-important role is the **Computer Fraud and Abuse Act**, or **CFAA**. **Read 18 U.S.C. 1030**.
- Section 1030(a) contains *seven* separate primary offenses (1030(a)(1-7)), some of which contain their own further subdivisions. Read each those provisions slowly, stopping after each one to (i) give it a short descriptive title that will help you remember its actual focus and (ii) try to create a very pithy list of the elements in each.
- Can you articulate the argument in favor of each of these provisions? Against any of them?
- Notice that the CFAA includes a clause creating liability for conspiracies and attempts to commit those offenses (1030(b)). Consider whether this gives rise to any potential problems.
- Notice, too, that Congress amended the CFAA in 1994 so that individuals could bring civil suits for some CFAA violations. Locate the relevant subsection of 1030, and decide when it applies. Was that a good idea or a bad one?

• 2. September 6 – Law Enforcement and Lawsuits

CFAA Criminal Charges in Practice

- The first big CFAA prosecution involved the ground-breaking—and largely accidental—"Morris Worm." **Read about the underlying events here**, and then **read the court opinion affirming his conviction here** (*United States v. Morris*, 928 F.2d 504 (2d Cir. 1991)).
- Do you agree that Morris violated the CFAA? Can you make the argument that this prosecution was desirable? Can you make the opposite argument? Which view is most persuasive to you? Would you alter the CFAA to produce a different result?
- The controversy surrounding the Morris case was nothing compared to that generated by the prosecution of Aaron Swartz. **Read about that here,** and then consider the same questions as above.
- **Read *United States v. Nosal***, 676 F.3d 854 (9th Cir. 2012) (en banc). Who was right: the majority or the dissent?
- The government on remand re-tried Nosal on a different theory: **read here** to see what happened next. What do you think of the government's revised theory?

CFAA Civil Suits in Practice

- Social media companies like Facebook and LinkedIn at times turn to the CFAA (using its civil liability provisions) in an effort to stop other companies from collecting information from public-facing parts of those sites. Whether and when such conduct violates the CFAA is a hot current issue. **Read about a current case involving Power Ventures and Facebook—one that might be considered by the Supreme Court this year—here and here**. Is this any different than the other cases we've read? Who should win?
- *HiQ v. LinkedIn* is a similar, recent case. **Read about it here and here**. Same questions as to the Power Ventures clash with Facebook.

Other Relevant Criminal Laws

- CFAA isn't the only tool in the toolbox for federal prosecutors dealing with cyber crime. There are some statutes of more-general applicability that often fit well with hacking scenarios, and there also are some highly-tailored statutes to consider. The most-relevant of the generally-applicable criminal laws, in this respect, is the "wire fraud" statute**. *Read 18 USC 1343***, and also ***read this article*** about a particularly interesting application of section 1343. What are the pros and cons of using this statute instead of the CFAA?
- Apart from "wire fraud," there are several other, more-specific fraud statutes. **Skim the following to get a sense of the options: 18 USC 1028** (identity fraud), **18 USC 1028A** (identity theft), and **18 USC 1029** ("access device" fraud).
- For a fascinating case showing how a variety of these statutes might be used, consider the prosecution of Roman Zeleznev (aka "Track2"). ***Read about it here***. This case turned out well for the government; do you think it indicates that similar success is possible in most such cases? Read this and this for a glimpse of some unusual complications.
- Note: There are other criminal laws that are important in this space, but that we will not explore in the interests of moving along to other topics. For the record, however, let's name a few of them: 18 USC 641 (theft of government property); 18 USC 2511 (unauthorized interception of communications); 18 USC 2701 (unauthorized accessing of stored communications); and 18 USC 793-798 (various provisions relating to espionage and protection of defense information). There also is 17 USC 1201-1205, aka the Digital Millennium Copyright Act ("DMCA"). We will study the DMCA in more detail in a later class).
- States have statutes analogous to the CFAA. For an overview of the relevant Texas statute, including observations on how it differs from CFAA in certain respects, ***read this***. For a sense of the state agency responsible for computer crime investigations, **read *here***.
- The United States is party to the "Budapest Convention on Cybercrime." ***Skim its provisions*** to get a sense of what it is trying to accomplish. Why do you suppose Russia, China, and Iran are not parties to it?

3. September 13 – Advanced Persistent Threats & State-Actor Challenges

Key concepts

- On "Deterrence" and "Cross-Domain Deterrence" in the cyberspace context, ***read this***. How many different tools---aside from a direct response of a like kind in cyberspace—might be available to the U.S. government in dealing with a state actor? Is the same true for other states? What about private actors? Should the government always make public that it has taken an action (in-domain or cross-domain) in response to another state's hacking? Can deterrence work without public claims of that kind? For a concrete illustrate, **read this**.
- On "Attribution" in the cyberspace context, ***read this and this***. Can you explain: why attribution matters, why it is thought by some to be especially difficult in the cyberspace context (and whether you agree), what such difficulty may mean as to decisionmaking in particular cases, and what such difficulty may mean as to larger questions of policy?

Russia

- ***Read this New York Times account*** from December 2016, which focuses on Russian election interference in 2016, and ***this one*** on possible responses. Questions to ponder: How did hacking in this context relate to a larger "information operation"? What lessons does this episode suggest about vulnerability to spear-phishing? How do you assess the response of (i) the FBI in particular and (ii) the U.S. government more generally? What insights did you gather regarding the entities that conduct such activities for the Russian government? How would you characterize what Russia did here (Crime? Espionage? Covert action? Some combination, or something else?)? What would you have done differently had you been president? And, finally, is any of this actually beyond the pale, in the sense that you would not want to see the United States doing the same thing (and do you see how that is a different question from asking whether the United States should do what it can to stop such actions from succeeding against it)?
- ***Read this Washington Post story*** regarding another Russia incident, ***the resulting indictment***, and the ***latest developments*** in the case. How do you assess the U.S. government response in this instance? Can the same model reliably be applied elsewhere?

China

- ***Read this Christian Science Monitor piece*** examining Chinese-government sponsored hacking against U.S. targets (public and private) in recent years. How does Chinese-government sponsored hacking differ from the Russian activities descried above, and what follows from this as a matter of policy? Should it be off-limits to hack businesses in hopes of providing competitive advantages for your own nation's companies (and does it really matter if the companies in question, on either end, are formally owned in part or in whole by the state)? Should the United States have done more to respond to these hacks?
- ***Here's a Foreign Policy piece*** with a slightly-different take on Chinese hacking. Does it change your analysis? Note it dates back to 2010, FWIW.
- The Obama administration surprised many observers when it brought criminal charges against a group of PLA hackers (*United States v. Dong* (W.D. Pa.). ***Read the indictment***, as well as ***this story*** and ***this story*** about the case. Analysis of the impact of this effort has been conflicted. ***Compare this account*** and ***this account***. What lessons if any do you draw from this? Is prosecution an effective approach? Scalable? Does news of ***this recent arrest*** – possibly linked to the famous OPM hack—change your view?
- Prosecution is not the only tool available, of course. ***Read this Executive Order*** from President Obama, which in April 2015 established a system for sanctioning the beneficiaries of cyberespionage used for commercial advantage. **Read more *here*** and ***here***, too.
- Eventually, the U.S. and Chinese government struck a deal, of sorts. What was it, and has it helped? ***Consider this analysis***. As for Russia, consider **this Dec. 2016 action**.

B. Encouraging Potential Victims[1] to Better Protect Their Systems:

Minimizing attack is not just a function of imposing painful consequences on attackers. It's also a function of making it harder for attackers to succeed (which both increases the cost to the attacker and reduces the likelihood of an offsetting return on their investment). Encouraging potential victims (private or public) to improve their defenses is thus an important sub-goal of cybersecurity policy.

Of course, most potential victims have at least *some* incentive to develop defenses even absent any form of government intervention. They have trade secrets to protect. They desire to keep things private. They need to keep customers happy. And so forth. As a result, there would be some defensive activity even if no external forces tried to encourage such steps. In that respect, it's rather like the situation of a building owner, who would take at least some steps to make the building safe even if there were no building codes, insurers, or plaintiff's lawyers. The question is, in both cases, would those steps be enough? We allow governments to intervene to spur further safety measures in the building-safety context, and increasingly we are doing the same with respect to cybersecurity.

As we shall see, the levers for intervention are pretty much the same in both contexts, at least at a high-level of generality (though it is much more interesting to study them in the cybersecurity context, since they are much newer and more-contested). There are three primary mechanisms, and we will spend one class on each of them in this subunit (as well as a fourth class examining some special circumstances associated with the *government* as the potential victim).

The first two mechanisms—regulation and liability—are familiar to most of us. In Class 4, we will examine the *regulatory* approach: that is, top-down imposition of rules (via statute or through regulations promulgated by an agency) that require certain entities to employ particular practices or procedures. In Class 5, we will turn to the *liability* approach: that is, creating exposure to suits for money damages or for penalties based on inadequate security practices (and, by extension, impacting the incentive-laden insurance industry too). Then, in Class 6, we will consider a subtle but important third mechanism: *removal* of barriers that undesirably deter better security. We will look at a case study of that "pruning" approach, involving the sharing of threat information.

Finally, in Class 7, we will look at the particular case of the government-as-potential-victim. This situation is a bit unusual from the regulatory perspective. On one hand, sometimes one government entity (say, Congress) may impose a top-down requirement on another government entity (say, some agency or department), in which case it feels analogous to regulation of the private sector. On the other hand, we not only see much more intrusive regulation in this setting (for government-regulation-of-government doesn't trigger the same political costs as does government-regulation-of-the-private-sector), but we also see situations in which the White House itself becomes involved in imposing requirements (via Executive Orders).

4. September 20 – Mandating Better Private Sector Defense: Regulators

[1] Note that "victim" is a tricky label in this context. At first blush, the "victim" of a breach is the owner/operator of the breached system. That breach might result in harm to customers or others, however, as in the case of a breach of a payment system that results in the exposure of credit card information. When we talk about victims in this context, therefore, bear in mind that there may be multiple layers of harm and thus both first-order and second-order victims.

The federal government contains a large number of administrative agencies. Each has some particular field of subject-matter responsibility (the scope of which is defined by statute in most cases). Each typically performs many functions, but we are especially concerned with two core capacities. First, an agency might have authority from Congress to promulgate legally-binding regulations relating to cybersecurity. Second, an agency also might have authority from Congress to initiate civil proceedings (either before an administrative law judge within the agency itself or in a regular federal court) to hold individuals or organizations accountable for violations of (i) federal statutes, (ii) regulations promulgated by the agency, or (iii) standards set by earlier enforcement proceedings. Question: Can such "enforcement" authority itself amount to a form of rule-making authority?

Federal Trade Commission

- For a very brief introduction to the Federal Trade Commission ("FTC"), read this. Based only on this overview, would you expect the FTC to have a role in setting or enforcing standards for cybersecurity? Why or why not?
- One of the statutes the FTC is empowered to enforce is the Federal Trade Commission Act. The FTC has not promulgated regulations under that heading relating to cybersecurity, but it has initiated more than 60 enforcement actions involving allegations of inadequate protection of customer data—many (though not all of which) involved allegations of poor cybersecurity. Can you explain why this effort can be viewed as having a larger regulatory effect?
- **Read** 15 U.S.C. 45(a)**(2)**, which is part of the FTC Act, to determine the set of persons or entities over whom the FTC has enforcement jurisdiction. Is the category limited to a particular industry?
- Now **look at both** 45(b) and 45(m) for an introduction to the two distinct procedures the FTC can use to take enforcement action. Can you explain the difference? In answering that question, consider both who decides whether the FTC's allegation is correct, and what remedies appear to be available.
- Of course, all this enforcement activity must involve allegations that some specific standard in the FTC Act has been breached. **Read** 45(a)(1) and 45(n) to see what that standard entails. What exactly is forbidden by this language? Though it is not a criminal statute like the CFAA, it nonetheless may be instructive for you to consider how it compares to the various CFAA provisions we mapped out last week. Would you say that the FTC standard is comparably clear?
- For an example of an FTC enforcement action within the FTC's own administrative process, **read** this complaint against Uber. What cybersecurity-related practices are alleged to have violated section 45(a), and assuming the fact allegations are true do you agree that this violated the statute? The case recently settled; **run a search** to see if you can determine what Uber agreed to do/not-do in order to satisfy the FTC.
- For an example of an FTC enforcement action involving suit in federal court, **read** this note summarizing the litigation involving Wyndham Hotels. Can you specify each argument Wyndham made against the FTC's claim, and as to each one can you explain both what actually happened and whether you agree with that outcome? Note: Wyndham and the FTC settled later, with Wyndham agreeing to take on a variety of security-focused practices (as well as annual audits) for the next 20 years.
- Compare the Uber and Wyndham Hotels situations to the FTC's ongoing case against LabMD, the twists and turns of which **can be read about** here. Is this case distinguishable from the others? What is the larger issue at stake? *(Optional: more on LabMD here.)*
- The FTC also has authority to enforce many other statutes, and in some cases to promulgate regulations relating to them. One such statute is the Gramm-Leach-Bliley Act (the "GLB Act"), which among other things concerns the protection of customer data by financial institutions. The FTC has promulgated a set of regulations on that issue, known as the "Safeguards Rule" (found in 16 Code of Federal Regulations Part 314). **Read** the text and also

this FTC-written overview, and see if you can explain what the rules require and whether this is different from the obligations under FTC Act section 45 as discussed above.
- For a recent illustration of the Safeguards Rule in action, **read** pp.3-5 of this action the FTC pursued against TaxSlayer. What actions/inactions did the FTC claim violated the Safeguards Rule, and do you agree with that assessment?

Other Federal Regulators
- There are other federal regulators involved in cybersecurity, besides the FTC. We will not go into the same level of detail with them, but you should have at least a glancing familiarity with the roles some of them play. For each example below, see if you can pin down the specific standard the agency is enforcing.
- **Read** here for an example involving the Securities & Exchange Commission ("SEC").
- **Read** here (just skim the first dozen pages) for an example involving the Federal Communications Commission ("FCC").
- Medical devices obviously raise especially-acute cybersecurity concerns, particularly when the device in question can be accessed remotely and is capable of causing significant harm. **Do some searching** to see if you can determine the extent to which the Food and Drug Administration (the "FDA") has gotten involved with cybersecurity regulations or enforcement as a result.

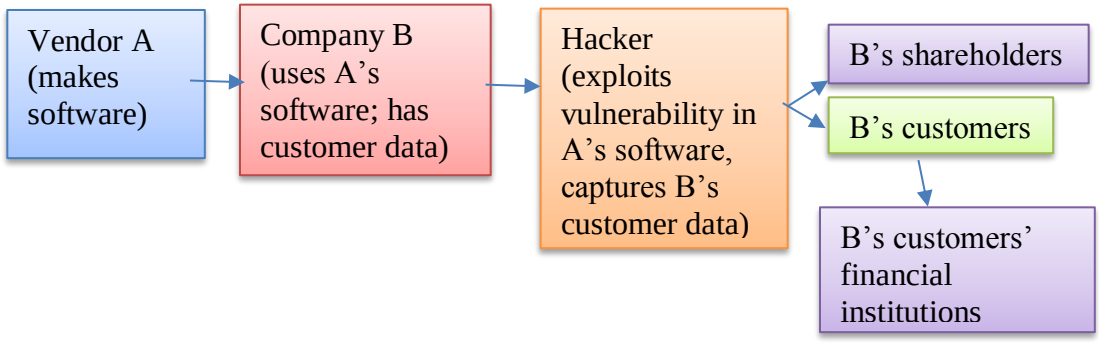
Don't Forget the State Regulators
- Why should it all be left to federal regulators? Actually, that's an interesting question: do you think it should be left to federal regulators? Regardless, state regulators also have gotten into this game. **Skim** this example, which recently took effect in New York in relating to the financial services industry. Is this helpful, or is New York State getting in the way of federal efforts (or, should both state and federal regulators back off)?

And Don't Forget the Foreign Regulators
- While we will not allocate time to studying any specific examples, you should be aware that some U.S. entities have operations overseas that may subject them to the cybersecurity-related regulations of other governments.

5. September 27 – Motivating Better Private Sector Defense: Litigation & Insurance

The Big Picture: Who Are the Injured Parties?

- Consider the following depiction of the chain of actors involved in a common type of cybersecurity incident:



- Consider who *might* count as the victims in this scenario. Obviously not the hacker. But which of the others might fairly be described in this way?
- One might expect that, if anyone is to be sued for damages, it would be the hacker. That rarely occurs, however. Why do you suppose that is?
- Suits are, in fact, very common in these scenarios. It's just that the defendant usually is not the hacker. Why not?
- Usually the defendant is not Vendor A, either, even if Vendor A's code contained significant flaws. Sometimes that is because Vendor A had already learned of a particular flaw and taken all reasonable steps to make available a patch to fix that flaw. But there are other reasons Vendor A typically will not end up as a defendant. **Read this article,** and see if you can enumerate the obstacles to suing software providers. Also consider how, if at all, you would change any of those obstacles.

Liability for Having Inadequate Security…or For Failing to Give Timely Notice of Breach

- In our legal system, we use the word "tort" to refer to wrongful actions/omissions for which an injured party can sue for damages. Generally speaking, torts are creatures of state common law (meaning that the particulars of a given tort may very a bit from state to state, and that the existence of the tort does not depend on a specific statute creating it (though there are plenty of statutes out there that do create civil liability for tort-like scenarios, as we have already seen with the Computer Fraud and Abuse Act at the federal level). At any rate, there is one common law tort in particular that has special relevance in the "inadequate security" scenario: Negligence. Negligence is perhaps the most familiar and fundamental of torts. As all law students learn during their first year, it makes a defendant liable in damages where four conditions are met: (1) the defendant owed a duty of care, (2) the defendant breached that duty, (3) that breach was the proximate (reasonably-foreseeable) cause of harm to the plaintiff, and (4) the plaintiff suffered harm for which a legal remedy (usually damages) exists. Pause now to consider how, in the scenario above, Company B's customers *might* have a negligence claim against (1) Company B and (2) Vendor A. (Note: The hacker, in this scenario, has likely committed not negligence, but one or more so-called intentional torts).
- For an example of a negligence suit filed without any evidence of an actual breach, where "Company B" was a *law firm*, **read this.** Taking each allegation as true, do you agree that each of the elements of negligence were satisfied?
- **Here is a complaint** against Equifax filed very soon after the recent breach was announced. Same question as above.

- Notice that in both these cases, the plaintiffs sought "class action" status. If granted, such status enables that single case to resolve the potential damage claims of all persons within the scope of the "class" of injured persons at issue. Consider the pros and cons of class-action status from the point of view of: the defendant, the plaintiff, and the plaintiff's attorneys.
- How does the standard of liability for negligence compare to the standard for liability under the FTC Act (15 USC 45(a)(1), and (for unfairness-based claims) also 45(n)) which we examined last week? Do the elements line up precisely?
- There is a variant of negligence known as "negligent misrepresentation," which as the name suggests amount to a claim of negligence based on the impact of a false or misleading statement on which someone relied. Bearing in mind the FTC Act "deception" cases from last week, can you explain how those same cases might have resulted in a negligent misrepresentation tort suit?
- Building on the last point, bear in mind that a company's security-related representations *might* appear in a "terms-and-conditions" document offered by the company to its customers as a set of conditions to which they must assent in order to access the company's services (just think of most of the apps you have installed on your phone). To the extent that such documents create a *contract* with the customer, the possible breach of such representations might also give rise to breach-of-contract suits from aggrieved customers. Indeed, the existence of a contract gives rise to a variety of possible breach-of-contract claims, as you will see in the next item…
- In February 2015, the health insurance company Anthem announced that its security had been breached and that a massive amount of personally-identifiable information about patients had been exposed. This led to massive litigation, illustrating not only the range of negligence and breach of contract theories plaintiffs might invoke, but a handful of other theories besides. Anthem tried to have these claims dismissed, but in early 2016 a federal judge rejected that effort. **Read the court's opinion** (*it is lengthy at 82 pages, but double-spaced; focus only on the parts that describe how specific theories of liability work, and whether the court felt the plaintiffs had made sufficient allegations to sustain those theories*). What additional theories of liability did you see, and do they seem to cover ground not otherwise covered by negligence and breach-of-contract?
- In reading the *Anthem* opinion, distinguish between claims based on Anthem's allegedly-inadequate security, and claims based on the way Anthem handled the aftermath of the breach once they knew about it. As to the latter: every state has a law requiring "Company B" to notify customers in the data-breach scenario, with slight variations as to the particulars. **Read this handy summary of the Texas law** for an example. How does Equifax look, so far as you can tell, under this law? Equifax delayed quite a long time before going public; can you think of reasonable justifications for that delay? Also note: some regulatory agencies also impose notification rules for companies within their jurisdiction.
- Back to the question of Anthem's liability for allegedly-inadequate security: Up to this point we have seen much talk of duties/standards of care with respect to data security. Have you considered how a lawyer would go about actually proving, with admissible evidence, whether a given security practice is up-to-standards? That question often is central in such cases, and as a result both parties frequently retain expert witnesses to testify on the subject. This, in turn, results in pre-trial litigation attempting to get the judge to bar the other side's expert from testifying. **Read this example** from the Anthem litigation.
- Anthem ultimately settled. **Read about it here.** What did the plaintiffs receive? What did the plaintiff's *attorneys* receive? How do you feel about this result, and by extension about the current system of tort liability for "Company B" in the event of a breach? Also **read this more-recent notice** about the settlement, and see if you see anything there about the impact of the settlement vis-à-vis "Vendor A," "hacker," and other entities mentioned in our scenario above.
- By this point, you surely are asking yourself: Didn't the regulators from last week also get in on the Anthem action? Of course! Last week we focused on the FTC, but also noted that many

other regulators might have a role depending on the industry of "Company B." In this case, a California state insurance regulatory agency got involved. The summary of its report is quite interesting, especially when read against the backdrop of the tort litigation and settlement described above. **Read the summary here.** Is this inconsistent with the civil litigation result? Is there a policy problem here, in light of the potentially-inconsistent results of the competing systems (regulatory, tort) we have been looking at this week and last? If you think there is…what would you recommend doing about it?

- Note the cryptic reference in the California insurance agency's report to the identity of the hacker responsible for the Anthem breach. Does it matter to your assessment of the Anthem breach that the hacker in question may have been Chinese government-sponsored hackers?
- You may be wondering whether the FTC got involved in pursuing Anthem. They didn't; instead, the Department of Health and Human Services ("HHS") did, for this was a breach exposing health-related information. For a quick glance at HHS's role in this space, **read this.**
- By this point, it should be clear to you that inability to prove financial harm, or at least to prove causation linking such harm to a data breach, is a recurring challenge for plaintiffs in this space. **Read this** for a critical perspective on that problem. Do you agree with EFF?

Shareholder Derivative Actions

- Recall that in our generic scenario above, we noted the possibility that Company B has shareholders who might sue it. Such "shareholder derivative actions" arise frequently with publicly-traded companies, when those companies experience any sort of significant reversal that might be attributed to bad decision-making by the company's officers or board of directors. **Read this article** for a fine overview of how such suits have fared in some of the most well-known data-breach cases. And be sure to note how the article illustrates the role that the "financial institutions" of "Company B's customers" might become involved as plaintiffs on a different theory.

Insurance

- In any context in which entities and individuals can anticipate suffering a loss—whether the loss be from damage to possessions or person, or from at least some forms of legal liability—there is a strong incentive to protect against the anticipated loss by purchasing an insurance policy. Because insurers usually (though definitely not always) are at liberty to determine which sorts of risks they will insure against, and subject to which conditions, the insurance industry in general is in a powerful position to nudge or even compel certain behaviors (just think of the incentives for safe driving that car insurance does or might generate). And thus insurance has an important role to play in relation to the general challenge of encouraging potential victim's to engage in better defense. For a handy and accessible (and brief) introduction to the emerging cybersecurity insurance market, **read this testimony** from a leading insurance executive before a Congressional hearing in July 2017.

6. October 4 – Removing Barriers: Information Sharing as a Case Study

Overview

We are in the midst of a subunit focused on ways to encourage better defensive practices. In classes 4 and 5, we looked at this from the point of view of external forces that pressure an entity to try harder. Specifically, we considered how regulators, plaintiffs, insurers, and contract partners all have various means of insisting upon improved security (either ex ante or ex post). But there's another perspective from which to consider this issue.

In some situations, an entity might be willing (perhaps even eager) to pursue some particular security measure, but is deterred from doing so by the potential applicability of a legal constraint. In such circumstances, "pruning" the law might be an effective means of incentivizing better security; think of it as addition-by-subtraction. The trick, of course, is that the law in question likely serves a competing interest, and hence potential security gains might come at a significant cost to other worthy values.

In this class, we will explore the "pruning" concept through a case study involving the removal of legal obstacles to sharing threat-related information.

An Introduction to the Problem and Key Institutions

- **Read** **this Congressional Research Service report**, from March 2015, in order to be able to answer the following questions:
  - What are the specific categories of information that might usefully be shared in relation to cyber threats? Do all of them likely include information that implicates privacy concerns?
  - One important form of information-sharing occurs between one private-sector entity and another. Before considering the *legal* obstacles to such sharing, see if you can identify any *non*-legal disincentives. Next, turn to the legal hurdles, which the report explores at some length. Be able to name and explain each of those hurdles, but also be able to identify the offsetting policy benefits that might justify having such a rule nonetheless.
  - What institutional mechanisms exist to facilitate private-to-private sharing? Can you explain what an ISAO and an ISAC are? To gather a sense of which industries have organized in those ways, **peruse** **this site** (maintained by the ISAO Standards Organization, run out of UTSA).
  - Now, consider cyber threat information sharing between the private sector and the government. Start by identifying as many relevant government actors in this space as you can, and the responsibilities/limitation of each.
  - Just like private-to-private sharing, private-to-government (and government-to-private) sharing involves both legal and non-legal obstacles. Once more, try to identify and make a list of the boundaries, including the justifications for having those limitations.
  - The CRS report mentions **Executive Order 13691 (President Obama, Feb. 2015)**. **Read** the actual order and determine whether it adds anything that the CRS report did not convey.

The Cybersecurity Information Sharing Act of 2015

- In 2015, Congress passed and President Obama signed a bill that included the "Cybersecurity Information Sharing Act of 2015" (generally known as "CISA"). The full text of that bill is here, but don't read the whole thing. Instead, let's look at specific provisions within it. **Use that link to read the following sections and answer the questions below for each:**

Section 103: What exactly does this section oblige DNI, DHS, DOD, and DOJ to do in relation to information-sharing?

Section 104(c): What legal limitation(s) does 104(c)(1) overcome? What is the point of the caveat in 104(c)(2)? And why include the language in 104(c)(3)?
Section 104(d)(1) and (2): What burden does (d)(1) create, and can you relate this to any of the existing duties/burdens we studied the prior two classes? What obligation does (d)(2) impose?
Section 104(e): Why was this provision necessary?
Section 105: This one is long. Review it carefully to decide what its most important functions are. Then **read this document** to understand how the agencies have responded to section 105. Does this leave you with any concerns?
Section 106: What legal obstacles does this section prune? Does it go too far, not enough, or just far enough?
Section 108(i) and (k): What are the effects of these provisions?

The FBI as a Micro-Case Study

- Pages **19-22 of this report by the DOJ Inspector General** provides important insights into the challenge of information sharing in the specific context of the FBI and the private sector (note: I posted the content of just those pages as a Word document on Canvas).

7. October 11 – Getting the Government to Protect Itself Better

In recent weeks we have surveyed the set of tools that government actors (agencies, legislatures, etc.) can use to incentivize (or even compel) private sector entities to adopt stronger security measures. But what about the government's *own* security practices?

The "government," of course, is a catch-all term referring to a vast array of distinct enterprises, any one of which may operate any number of separate networks, databases, etc. Even if we limit our focus to the U.S. government (leaving aside states, counties, cities, tribal governments, territorial governments, and so forth), the number of relevant actors is bewildering. Like the private sector, these entities have internal incentives to maintain the security and functionality of their systems (the SEC does not want people to access private information and thus enable market manipulation, just as NSA does not want Russia to be able to learn its techniques and capabilities). But also like the private sector, we have ample reason to believe that, if left to their own devices, plenty of government entities either would not—or perhaps could not—invest as much in security as they should.

Our goal this week is to understand how the ecosystem of external incentives for government actors is different from what we've seen in the past several classes in relation to the private sector. Towards that end, we'll use the infamous data breach at OPM—the Office of Personnel Management—as a case study.

1. Background: The OPM hack as a case study

- The most well-known data breach involving a U.S. government system involves the hugely-successful operation through which Chinese hackers breached security at the Office of Personnel Management, acquiring a vast trove of security-clearance background check files. Congress conducted an extensive investigation, resulting in publication of a massive report documenting how the breach occurred. I have posted an edited version of that document (still lengthy at 96 pages) on Canvas, and would like you to ***skim* the excerpt** (I'm reluctant even to link to the full 241-page document, but here it is if you want to explore further) both to have a sense of what happened and also to answer the following questions:
    - How did the attackers gain access to OPM's systems, from a technical perspective?
    - The authors of the report clearly feel that OPM should have had better security (i.e., this wasn't just a matter of a skilled and well-resourced adversary getting lucky). But why do they think that? See if you can identify specific factors that might explain OPM's failure. For each factor on your list: Was it a failure of policy? Law? Management? Budget? Job performance?

2. Do government entities have to worry about lawsuits?

- As we have a seen, a private sector entity must take seriously the prospect of various forms of financial harm should it fail to invest adequately in security. It might face an enforcement action from a regulator (like the FTC), it might find that it lacks insurance, and it might find itself on the wrong end of a lawsuit seeking damages. That trio of incentive-making considerations has relatively little impact on a government entity, however.
- To some extent, the reasons why this is so are obvious. For example: regulatory agencies like the FTC do not initiate investigations and enforcement actions against other government agencies, and government agencies do not rely on insurance in the manner of a private entity. But what about litigation risk? The federal government faces comparatively little

litigation risk in comparison to a private sector entity, because (as a default matter) it enjoys "sovereign immunity" from suit. This means that the government can only be sued insofar as it has "consented" to be sued, typically in the form of legislation authorizes suits against the government in specific circumstances.

- Are there statutes that provide such consent in contexts relevant for cybersecurity? A case arising out of the OPM fiasco provides a convenient illustration both of the legal theories plaintiffs might put forward in such a case, and the reasons they usually will fail. **Read pages 53 to 67 of Judge Amy Jackson's opinion** in *In re: U.S. Office of Personnel Management Data Security Breach Litigation* (D.D.C. Sep. 29, 2017) (note: the PDF version I posted to Canvas is edited so as to give you just the first page plus pages 53-67). Be prepared to answer:

    - What does the Privacy Act bar the government from doing, and why did Judge Jackson conclude that this standard was not met in the OPM scenario?
    - What does the Little Tucker Act (yes, you read that name correctly) prohibit, and why did that argument fail here?
    - Why did the plaintiffs think the Administrative Procedures Act (the "APA") could help them, and why did that argument fail?
    - What constitutional right did the plaintiffs attempt to invoke, and why did that argument fail?
    - The final page of the excerpt (p.67 in the original) includes the start of the court's analysis of a separate set of claims that were brought against a private contractor that had been working with OPM. Note the court's reference to the idea of "derivative" sovereign immunity. The idea is that the government's sovereign immunity extends to its contractor so long as the contractor's actions are within the terms of the contract and do not otherwise violate federal law.

3. Self-Regulation: Using Statutory Mandates and Executive Orders to Make Agencies Try Harder

- The preceding discussion makes it sound as if government entities might just be left to their own devices (in terms of deciding how much effort to put into security). But that's not really the case, for both Congress and the President have intervened in certain ways in hopes of driving government agencies to put more care into the security of their networks.
- In 1996, Congress passed the Information Technology Management Reform Act (Pub. L. 104-106), which included a provision (section 5131) directing the Secretary of Commerce to promulgate information-security standards that the rest of the government (except for defense and intelligence agencies) would have to follow (barring intervention from the President). The statute specified that the Secretary should base his or her directives on the standards and guidelines developed by the Commerce Department's National Institute of Standards and Technology (better known as "NIST").
- In 2002, Congress passed the Federal Information Systems Management Act of 2002 ("FISMA"), which among other things effectively transferred the Secretary's responsibility over to the Director of the Office of Management and Budget (OMB). The stated purpose of FISMA is, among other things, to: "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets," including development and maintenance of *minimum controls required to protect*" those resources while recognizing that "selection of specific technical hardware and software…solutions should be left to individual agencies." Towards that end the Director of OMB was supposed to

    - develop common policies and procedures to assist those agencies
    - review agencies' information security programs at least once a year
    - report to Congress on agency compliance

- oversee a "Federal information security incident center" to serve as both an expert resource to assist the agencies (especially in the midst of an incident) and to provide a central hub for collecting and analyzing threat information).

- In the years that followed, the "Federal information security incident center" concept became US-CERT ("Computer Emergency Response Team"), which as we noted last week is part of DHS's NCCIC today. Of course, DHS itself did not exist that the time of the original 2002 FISMA. Once DHS was established, however, it became a natural home for the executive branch's growing focus on cybersecurity.
- In 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (available here, though you need not read it in full). NSPD 54 confirmed the lead role of DHS in protecting federal networks. Among other things, it directed DHS to act through US-CERT to monitor and protect all "external access points" associated with federal government systems, and to provide intrusion detection, incident analysis, and other capabilities
- Over time, DHS has developed various iterations of intrusion-detection and mitigation services under the label of "Einstein." Here is an account of Einstein 2 and Einstein 3, from the Obama Administration (full source here, but you can just read the excerpt below):
  - …DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting Internet traffic entering Federal systems for unauthorized accesses and malicious content. The EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology. … EINSTEIN 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data. [Meanwhile, DHS is developing a new system], called EINSTEIN 3, [that] will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. … The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions. … DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission. Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens.
- In 2010, OMB formally delegated the oversight component of its FISMA role to DHS, while keeping its role in promulgating NIST-based standards for agencies to follow. In 2014, Congress confirmed this arrangement by passing an updated version of FISMA. Pursuant to 44 USC 3553:

  - The OMB Director shall continue to have its existing role in promulgating policies and guidelines (based on NIST standards) for all federal agencies (other than those operating national security systems).

  - The DHS Secretary shall have authority to issue "binding operational directives to agencies" to make them comply with the OMB Director's policies and guidelines, and to monitor for compliance.

- Pause now to consider whether this review of federal efforts to boost federal agency security changes your views regarding the lessons to be drawn from the OPM fiasco (or, conversely, whether the OPM fiasco changes your assessment of these federal efforts).
- In May 2017, President Trump issued an executive order addressing federal agency cybersecurity, as well as other matters. **Read just section 1 of the order, here**, and determine

what, if anything, this changes from the status quo (and to the extent you do see a change, form an opinion on whether it is useful). Hint: What does "accepted risk" mean?

C. Managing Consequences

Even if we have strong incentives for potential victims to take protective measures, and even if we severely discourage potential attackers, some amount of harm still will occur (and those are both rather big "ifs," so it may be more accurate to say that a *large* amount of harm will still occur). What then?

We will round out our survey of the defensive perspective with a two-class sequence on consequence management.

Breaches come in all shapes and sizes, of course, and in many instances the consequence-management scenario is simply a private matter for the victim involving the sort of regulatory, litigation, and insurance problems discussed above (in some cases compounded by public-relations challenges, if and when the matter becomes public). But sometimes the scenario has wider significance. Sometimes the harm is sufficiently widespread or complicated that special forms of cooperation are required to mitigate it. In Class 8, we will examine responses to breaches and botnets. Separately, some victims are considered "critical infrastructure," and in other cases the sheer nature of the attack—or the identity of the attacker—may in any event elevate the situation into a matter of national concern. In Class 9, we will examine the various institutions, policies, and issues that might arise in such cases.

8. October 18 – Responding to Breaches and Botnets

Up to this point in the course, we have focused on situations in which breach of security allows an unauthorized person to acquire valuable data (e.g., Equifax or OPM). In some situations, however, the point of unauthorized access is not to extract confidential information from a compromised system, but rather to put the compromised computer to work on some task without the computer's owner knowing it. All the better, of course, if this can be done at scale. This leads us to the topic of botnets.

About botnets

The ability to put a compromised machine to work surreptitiously can be valuable to an attacker in two ways. First, a compromised computer can be used in ways that earn money, such as sending out spam, engaging in pay-per-click advertising fraud, or mining Bitcoin. Second, a compromised computer can be used to as a weapon of sorts, sending traffic to some site that the attacker hopes to overwhelm and thereby deny service to its legitimate users. Both approaches require scale to be worthwhile. That is, both are worth the attacker's trouble only if the attacker can compromise and put to work a large number of machines. Thus the attractiveness of assembling a "botnet."

By botnet, we are referring to the situation in which an attacker (the botnet "herder") has compromised a large number of computers and can put them all to work on the sorts of tasks described above. Here's the general idea:

a. There is a vulnerability in some widely-used software.

b. Someone develops malware capable of (i) exploiting that vulnerability in order to deliver a payload to infected machines and (ii) spreading rapidly to other machines.

c. The payload delivered by the malware might be static in the sense that it simply directs the compromised machines to perform whatever function the attacker originally had in mind, and does not include the capacity to receive new commands. More commonly, though, the payload is dynamic in that it enables the attacker to issue updated commands to compromised machines on an ongoing basis, via one or more external servers (the "command-and-control servers") which the attacker controls.

d. The herder who assembles the botnet can put it to work for his or her own purposes, or (as we saw in Week 1) can sell access to the botnet (on a temporary or permanent basis) to others.

Botnets present several distinct policy challenges. We will focus on two of them. The first one is simply a continuation of the theme we have been exploring for several weeks: How to encourage better information security practices by the owners of individual computers (thus making it harder for botnets to form in the first place)? The second changes perspective from prevention to remediation: How to take down a botnet once it forms?

Challenge #1: Making it harder for botnets to form in the first place

Viewed in isolation, the harm that might result from the vulnerability of any single personal computer is likely to be relatively limited (though no doubt quite serious for the owner of that computer). The scale of the harm a botnet can cause, however, puts the vulnerability of individual computers in a different light, and obliges us to consider what steps might be taken to encourage everyone—all of us who own computers—to take more care when it comes to our own cybersecurity practices.

To grapple with that question, it helps to have a sense of why individual computers so often are so vulnerable. **Read** this article to gather a sense of the security challenge associated with software vulnerabilities impacting laptops and the like, and answer these questions:

1. Why don't people keep the software on their computers/devices up to date?

2. Can you think of any way to address this problem through technology? Through negative incentives? Through positive incentives?

3. Change your focus from the owner of unpatched/outdated systems, and think instead about entities that might be in a good position to know that a given individual computer is vulnerable (or perhaps even already compromised). Which entities are in such a position already, and what in theory might they be able to do in such cases? Any reasons (legal, technical, policy, business, or otherwise) why we should be hesitant to encourage such entities to play this kind of role?

4. Did you notice that the malware at the center of that story did not serve to create a botnet, but instead was ransomware? Above I suggested that compromise of computers belonging to individuals for purposes of extracting valuable data generally did not amount to a significant public-policy challenge. This arguably was true in years past in relation to ransomware, too. If it ever was true, though, is it still true now?

Now let's complicate the picture a bit more by highlighting the way that the Internet of Things ("IoT") aggravates the botnet challenge. IoT refers to the rapidly-increasing number of devices (in and out of the house) that are web-enabled; that is, things that we don't normally think of as

computers (from refrigerators to pacemakers) now have connectivity and can be compromised. There are many benefits that come from such connectivity, but unfortunately it also means IoT devices can be hacked—and if they can be hacked they can be added to a botnet. Alas, IoT devices turn out to be particularly-ripe for hacking. **Read** this article to develop your understanding of the dynamics involved in this problem of ubiquitous vulnerability. Be able to answer:

5. What factors account for the fact that IoT devices so often are vulnerable? Consider, for example, whether there are problematic (but common) practices of manufacturers in relation to passwords and patching, and also give thought to whether the purchaser of an IoT device is much incentivized to spend time trying to enhance the security of those devices (or to consider relative security when making the decision to buy a particular device in the first place).

6. Manufacturers don't want their IoT devices to be exploited. What business factors explain why they nonetheless so often have such poor security?

So, can anything be done about the IoT vulnerability problem? There is a bill currently pending in the Senate called the Internet of Things (IoT) Cybersecurity Improvement Act of 2017, aspiring to help address this problem. **Read Section 3(a) of that bill**, and be prepared to answer:

7. What is the function of this section?

8. Would it have any impact outside of government?

The bill goes on in sections 3(b) and 3(c) to propose some legal "pruning" that might help generate better IoT security. You will read those sections in a moment, but first there is some context concerning "security research" that will help you appreciate them. Security researchers—also known as "ethical hackers" or "white-hat hackers"—are information security professionals who use their skills to identify vulnerabilities and exploits not in order to make use of them, but rather in order to induce the relevant vendor to address them and thereby improve the security of their products. Enlightened vendors often will pay for such information, pursuant to "bug bounty" programs run either directly by the vendor itself or through third-party companies that broker such arrangements. Other vendors can have idiosyncratic reactions when approached by a security researcher, and still others have quite negative reactions—including threats of legal action under the Computer Fraud and Abuse Act or under statutes that protect intellectual property rights. The latter prospect casts a considerable shadow across the security research industry. For an excellent introduction to those challenges, **read pp. 39-55 of** this article (Ido Kilovaty, Freedom to Hack **(2017))** (note: the version posted to Canvas is edited to leave out all the other pages, whereas this link to the original will give you the full (lengthy) document)). *(Optional: if you would like to learn more about the "bug bounty" industry, you will enjoy this podcast interview)*

9. What values are served by the DMCA?

10. Why do people think the DMCA as a default matter might deter security research?

11. What exceptions are built into the DMCA, and why are they not a sufficient solution?

12. What role does the CFAA play here?

Now, back to that bill aimed at improving IoT security. **Read sections 3(b) and 3(c)**.

13. How would these subsections address the concerns of security research?

14. Once security researchers discover a vulnerability, an important question arises about the process of informing the vendor or the public about it. Why might we wish to discourage researchers from immediately going public with information of this kind, if they wish to do so? On the other hand, why might we want to avoid a situation where disclosure is left entirely to the vendor?

15. How does this bill try to manage the process?

Challenge #2: Dealing with botnets after they have formed

Botnets happen. And they will continue to happen even if we make considerable strides in improving the aggregate level of security for connected devices. So we must also pay attention to the process of mitigating the harm from botnets once they form. The ultimate question is: How do we destroy them?

Over time, the FBI, the Justice Department (CCIPS), and the private sector (both vendors and scholars/researchers) have honed a process for "botnet takedowns." Our goal in the second half of class this week will be to understand who the key players are in this process, what the challenges (policy, legal, business, and technical) are, and how the process has evolved over time.

Read this article from Wired regarding the takedown of the GameOver Zeus botnet. Then, **read this "Memorandum of Law in Support of Motion for a Temporary Restraining Order."**

16. What were the respective investigative roles of the FBI, the private sector in the United States, and foreign partners?

17. From a practical perspective, what did it take to take down the botnet?

18. Why was it necessary to involve the courts in that process? What legal theory(ies) did the government invoke to get those orders?

Finally, **read this** explanation from the Justice Department regarding a change it sought involving Rule 41 of the Rules of Criminal Procedure, which became law not long ago. Then see this example of a Rule 41 warrant relating to the recent Kelihos botnet takedown.

19. Warrants normally involve judicial approval to arrest someone, to conduct a search of some location, or to seize certain things. What role does a warrant play in the setting of a botnet takedown?

20. How does the new Rule 41 assist, and why might this be controversial?

9. October 25 - Defense in Special Contexts: Critical Infrastructure and "Significant Cyber Incidents"

Not all cybersecurity incidents are equal. Some threaten more harm than others, as in the case of breaches that might enable disruption of "critical infrastructure" (hereinafter "CI").

In anticipation of such cases, we might expect the government to take special steps to encourage CI owners and operators to improve their security in hopes of preventing incidents in

the first place. And we also should expect government to take on a more-active-than-normal role in the event an incident involving CI (or otherwise counting as a significant cyber incident) occurs.

Context

To place the policy challenge in context, we begin with accounts of recent episodes involving cybersecurity threats to CI. **This Symantec report** from last month provides a technical account of recent intrusions involving the energy industry, and **this Wired article** provides further useful context for that report. **Another Wired article**—this one from June 2017—goes into detail about especially-significant Russian cyberattacks on the Ukrainian electrical grid, illustrating what might be possible in a worst-case scenario.

Next, let's also note a factor that complicates the project of encouraging better defense in the CI context: much if not most CI in the United States is privately-owned.

> *1. Why, exactly, does the fact of private ownership "complicate" the task of spurring better defense? Put another way, why should we think this task would be easier if the government controlled CI directly?*
>
> *2. Are there any cybersecurity advantages that might flow from private ownership of CI?*

Early efforts to improve cybersecurity relating to CI

Federal efforts to address cybersecurity threats relating to CI go back several decades. We will not explore the earlier part of this history, but you should at least be aware that the Clinton and George W. Bush administrations were aware of this issue, and took a variety of initial steps in response to it. Having said that, our own study of this topic jumps in with a pair of actions by the Obama administration in February 2013.

First, let's look at the Executive Order President Obama issued that month. **Read the following sections from Executive Order 13636** ("Improving Critical Infrastructure Cybersecurity"):

Section 2

> *3. What is the definition of CI offered here?*
>
> *4. Is this a proper definition? Consider whether it is over- or under-inclusive, and whether it is sufficiently clear (bearing in mind there may be both costs and benefits to ambiguity and vagueness).*

Section 4(c), (d), and (e)

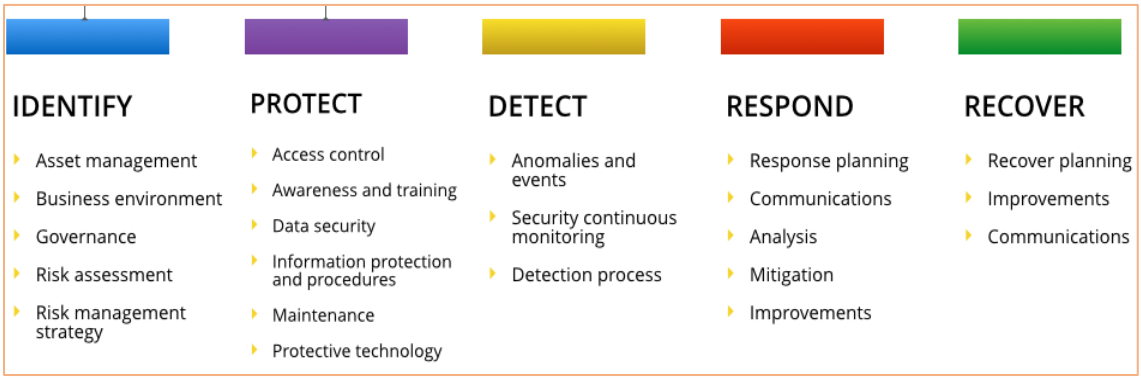
> *5. We previously studied the general mechanisms for sharing cyber threat information. What is distinctive about 4(c)?*
>
> *6. How does 4(d) help 4(c)?*
>
> *7. Can you think of an example of how 4(e) might work?*

Section 7(a) and (b): These sections directed the Commerce Secretary to have NIST create (and keep updated) a "Cybersecurity Framework" designed to help CI owners "to reduce cyber risk." NIST has since published version 1.0 of the Cybersecurity Framework, and a version 1.1 is in the works at this time. Here are some key excerpts

from version 1.0, designed to help you understand what the Framework does—and does not—aspire to do:

> "The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management.... The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. … The Core is not a checklist of actions to perform…."

The following graphic captures the "core" of the Framework, giving you a more-specific sense of how the Framework really is a form of comprehensive risk-management guidance:



Note that under each of these categories and subcategories, the Framework goes on to cross-reference a wide variety of more-specific standards that might be relevant.

8. How (if at all) is this useful?

9. Section 7(b) specifies that the Framework should be "technology neutral." Does this remind you of any prior discussions? Think of the FTC and the debate surrounding the generality of the FTC Act.

Section 8(a), (d), and (e)

10. Does the Executive Order purport to make private sector CI owners legally obligated to adhere to the Cybersecurity Framework?

11. Can such obligations be created, directly, via Executive Order?

12. Does the existence of the Framework nonetheless cast a legal shadow of sorts, one that might create incentives for CI owners?

13. Focus on (d) and (e): how do those provisions aspire to increase uptake of the Framework model?

Sections 9 and 10 Section 9 calls for identification of especially high-risk CI. Section 10 calls for those federal agencies that happen to have regulatory authority over various kinds of CI owners (think, for example, of a nuclear power plant and its relation to the Department of Energy) to review the sufficiency of their regulations pertaining to cybersecurity, with special regard to CI owners listed pursuant to Section 9. Section 10 adds that if an agency concludes it needs greater regulatory authority in this area, it should say so. It also requires agencies to report on the possibility of *over*-intrusive regulations.

Section 12

14. Focus on the second sentence. Why is it there, and how does that pertain to the note above regarding Section 10?

On the same day that President Obama issued EO 13636, he also issued **Presidential Policy Directive 21** ("PPD-21") (it is available here if you are curious, but you do not need to read it). We will focus on two aspects of PPD-21.

First, PPD-21 directed DHS to establish twin, coordinated offices focused on information and analysis relating to CI, including a capacity for near real-time situational awareness of unfolding events impacting CI owners and operators. The following quote from a DHS explanatory document (if curious you can see the full thing here) unpacks the confusing nomenclature for the resulting offices (one of which—NCCIC—we have studies before in the information-sharing context):

"The National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) fulfill this Department of Homeland Security (DHS) responsibility within the critical infrastructure partnership. This supplement describes how partners throughout the critical infrastructure community…can connect to the NICC and NCCIC. …

These centers, along with an integrated analysis function, build situational awareness across critical infrastructure sectors based on partner input and provide information with greater depth, breadth, and context than information from any individual partner or sector. …

1. The Centers

The National Infrastructure Coordinating Center (NICC)

The NICC is the watch center component of the National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (IP), the national physical critical infrastructure center designated by the Secretary of Homeland Security, and an element of the National Operations Center (NOC). It is the national focal point for critical infrastructure partners to obtain 24/7 situational awareness and integrated actionable information to secure the Nation's physical critical infrastructure. When an incident or event impacting critical infrastructure occurs that requires coordination between DHS and the owners and operators of critical infrastructure, the NICC is the national coordination hub to support the security and resilience of physical critical infrastructure assets. The NICC collaborates with Federal departments and agencies,

SLTT governments, and private sector partners to monitor potential, developing, and current regional and national operations of the Nation's critical infrastructure sectors.

The National Cybersecurity and Communications Integration Center (NCCIC)
The NCCIC is the lead cybersecurity and communications organization within DHS, serving as the national cyber critical infrastructure center designated by the Secretary of Homeland Security. It applies analytic resources; generates shared situational awareness; and coordinates synchronized response, mitigation, and recovery efforts in the event of significant cyber or communications incidents by regularly coordinating with law enforcement, the Intelligence Community (IC), international computer emergency readiness teams, domestic information sharing and analysis centers (ISACs), and critical infrastructure partners to share information and collaboratively respond to incidents."

15. Can you explain the difference between those two centers?

16. Do we need both?

Second, PPD-21 identified 16 CI "sectors" of the economy, pointing out for each sector which federal agency normally shall play a leading role (the "sector-specific agency," or "SSA"). PPD-21 directs the Secretary of Homeland Security to reconsider the list periodically as needed, adding or subtracting as needed (subject only to advance consultation with the Assistant to the President for Homeland Security and Counterterrorism). PPD-21 explains that CI for this purposes means "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." (This somewhat-awkward formulation is borrowed from 42 USC section 5195c).

17. Are you satisfied by this definition of CI?

18. If not, what would you change?

Review the current list of **16 industry sectors** that count as CI, and note that DHS in January **added election systems** to the roster.

19. Do you agree that all belong in the CI category? And is there anything missing?

20. Note that DHS Secretary Jeh Johnson felt obliged to emphasize the limited impact of adding election systems to the CI list would have.

a) What policy objections to such a designation might there be?

b) What are the politics of this question?

c) What factors does Johnson cite to ameliorate the policy concerns? (Note: this is an especially-important question, as it gets directly to the larger question of whether and how it matters to receive a CI designation)

d) Should we be concerned, in light of your answer to the last question, that the federal government is not doing enough?

21. Is Hollywood critical? It's not a rhetorical question, it turns out. The question arose in public debates after North Korea's famous hack of Sony Pictures (the hack was punishment for releasing "The Interview," a mediocre comedy featuring Seth Rogen and James Franco tasked with assassinating North Korea's leader). Did the breach amount to an attack on CI? ***Using the "16 industry sectors" link above, find your way to the "Commercial Facilities Sector-Specific Plan."*** *This is a highly-detailed document produced by DHS to flesh out the rationale and particulars defining the various CI sectors.* ***Use that document*** *to decide whether the Sony Hack counted an attack on CI under the DHS definition.* ***Next, refer back*** *to the definition of CI used in PPD-21 and 42 USC 5195c. Do you feel that the Commercial Facilities Sector-Specific Plan adheres to that definition?*

New efforts in 2016

In July 2016, the Obama Administration issued PPD-41, titled "United States Cyber Incident Coordination." **Read** the sections as indicated below:

Section II

22. What is the difference between a "cyber incident" and a "significant cyber incident?"

23. Why draw that distinction?

24. Ponder the definition of "significant cyber incident." Is it sufficiently clear so as to yield predictable answers as to which incidents fall into that category?

Section IV

25. Can you explain the difference between and among "threat response," "asset response," and "intelligence support/related activities"?

26. In practical terms, what specific forms of federal government involvement does Section IV suggest will occur with run-of-the-mill cyber incidents?

Section V – This section applies only to "significant cyber incidents."

27. What is the difference between the Cyber Response Group and the Cyber Unified Coordination Group? ***Read Section II.A. of a separate document—the "Annex" to PPD-41—****to understand who sits on the CRG and what it should do. Then* ***read Section II.B of the Annex*** *to understand more about the Cyber UCG concept.*

28. Why do we need either of these in relation to "significant cyber incidents," but not run-of-the-mill "cyber incidents"?

29. In Section V(c), certain responsibilities are placed on the FBI (in coordination with the National Cyber Investigative Joint Task Force organization, which FBI leads), DHS (in the form of NCCIC), and the Office of the Director of National Intelligence (through its CTIIC). How if at all is this different from what would occur if an event was merely a "cyber incident"?

Note that the last part of the Annex to PPD-41 directed DHS to work with others to create a "national cyber incident response plan" within six months. In December 2016, DHS accordingly

published **The National Cyber Incident Response Plan.** The full version is available here, but I'm only interested in having you **read the section on "Operational Coordination During a Significant Cyber Incident," which starts on p. 29 and ends on p. 35, plus Annex B on p.38** (the version in Canvas is edited to just be those pages, plus the cover)

> *30. The NCIRP sheds additional light on when an incident counts as "significant." How so, and did you find this useful?*
>
> *31. You have seen how both PPD-41 and the NCIRP empower certain entities to take a lead role in terms of threat, asset, and intelligence response. Would you add or subtract anything from this arrangement, and if so would you make that change as to all significant cyber incidents or only upon satisfaction of certain conditions? That's another way of asking: Do we need further gradations of severity in order to enable different default rules for lead agency responsibility and mandatory decision-making and coordinating processes?*

The 2017 Executive Order from the Trump Administration

In May 2017, President Trump issued **Executive Order 13800 ("Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"**). In an earlier class we read portions of it dealing with the task of improving the security of federal systems. Now we look at what it has to say about protection of CI. **Read the following subparts of Section 2 of EO 13800,** and consider the following questions:

> **Section 2(b)** This subsection gives DHS six months to investigate the prospects for the federal government to do more in relation to protecting the CI entities identified under "Section 9" of EO 13636 (Feb. 2013) (see above to remind yourself what that means).
>
> > *32. What do you suppose the drafters had in mind here as a possibility, and what obstacles might arise?*
>
> **Section 2(c)** This subsection calls for study of "market transparency of cybersecurity risk management practices by" CI entities, especially the public-traded ones.
>
> > *33. What is this about, and how might pressure in this area help spur better security practices? (*Note: this report appears to be done around November 11th, though it might be classified.)
>
> **Section 2(d)** This one concerns the botnet problem we studied last week.
>
> > *34. Is this section proposing a particular solution, or just urging further study?*

Going forward?

You will have noticed, by now, that none of the documents reviewed above has attempted to address cyber threats to CI by having a government entity—the NSA, CYBERCOM, etc.—actually take on the direct responsibility for monitoring networks and performing security functions directly on behalf of private entities. We might see such a proposal at some point, however (*cf.* question 32 above).

35. List the pros and cons of empowering NSA or other government entities to take on such a role.

It would be a mistake to assume that the Defense Department actively seeks such a mission. Consider this excerpt from the written testimony of a Defense Department official, before the Senate Armed Services Committee, in October 2017:

> STATEMENT OF MR. KENNETH RAPUANO
> ASSISTANT SEC. OF DEF. FOR HOMELAND DEFENSE & GLOBAL SECURITY
>
> TESTIMONY BEFORE THE SENATE ARMED SERVICES COMMITTEE
> OCTOBER 19, 2017
>
> …Although DoD has built capacity and unique capabilities, for a number of reasons, I would caution against ending the current framework and against reassigning more responsibility for incident response to the Department of Defense.
>
> First, DoD's primary mission is to provide the military forces needed to deter war and to be prepared to defend the country should deterrence fail, which requires us to be prepared at all times to do so. DoD is the only department or agency charged with this mission, and success in this requires the Department's complete focus. In this case, any significant realignment of roles and responsibilities will have opportunity costs, including absorptive capacity to build mission capability in a new area, especially ones that could distract the Department from its core warfighting missions.
>
> Second, the United States has a long normative and legal tradition limiting the role of the military in domestic affairs. This strict separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions. Designating DoD as the lead for the domestic cyber mission risks upsetting this traditional civil-military balance.
>
> Third, a primary civil reliance on DoD in the steady-state would result in increased demands that could not be met without significant changes in resource allocation. We would expect even greater demand in a conflict scenario, when there might be a natural tension in the need to preserve DoD mission capabilities and requests for support to civilian agencies. Even with such a change in resource allocation, the addition of a new mission would likely detract from the focus on and readiness for the warfighting mission.
>
> Finally, putting DoD in a lead role for cyber incidents creates an exception to accepted domestic response practice in all other domains, which would disrupt our efforts to establish and maintain unity of effort. Civilian agencies have the lead responsibility for domestic emergency response efforts; this should not be different for cyber incidents. The Federal Government should maintain a common approach to all national emergencies, whether they are natural disasters or cyberattacks.

36. Does this change your analysis?

Is there a "third way" alternative? Consider this concept, advanced by then-Deputy Secretary of Defense William Lynn in a speech in 2010:

> "Years of concerted investments on the military side have placed critical cyber capabilities within the Defense Department and National Security Agency. We are already using our technical capabilities to support DHS in developing the Einstein 2 and 3 programs to protect government networks. We need to think imaginatively about how this technology can also help secure a space on the Internet for critical government and commercial applications.
>
> For the .com world, could we create a secure architecture for that lets private parties opt-in to the protections afforded by active defenses? In this way protection would be voluntary. Operators of critical infrastructure could opt-in to a government-sponsored security regime. Individual users who do not want to enroll could stay in the "wild wild West" of the unprotected Internet. This type of secure.com approach could build on the collaboration between DoD and the defense industry. It could offer an important gateway to ensure our nation's critical infrastructure is protected from cyber attacks."

37. What are the pros and cons of this bifurcated model?

II. THE OFFENSIVE PERSPECTIVE

In the second half of the course, we will turn our attention away from the institutions, laws, and policies that promote defense and towards the limited set of circumstances in which our institutions, laws, and policies promote (or at least tolerate) *offense*. That is to say, we will be concerned with situations in which it (arguably) is desirable to promote efforts to penetrate or interfere with a system without its owners authorization (or, perhaps, awareness). For the sake of convenience, we might call this lawful-but-unauthorized access (meaning lawful from a U.S. perspective…needless to say, such activity overseas may well violate the laws of other countries).

You will note immediately, I hope, that the very idea that we would have a category of lawful-but-unauthorized access is in considerable tension with the policy goals advanced by, well, pretty much everything we studied in Unit I. Why, then, should there be such a category? We will explore that policy question across several contexts.

First, in Week 10, we will consider the counterintuitive notion that this can actually promote security. That's the theory of those who advocate empowering the private sector, when attacked, to defend itself by taking measures that have effects outside their own networks (especially, but not necessarily only, in the network of the attacker). Next, in Week 11, we will consider "lawful hacking" conducted by law enforcement investigators (a topic that also requires a foray into the fierce disputes surrounding the "Going Dark" debate—*i.e.*, the fight over whether Congress should require companies to preserve the ability to execute search warrants on encrypted devices or platforms, at a time when many companies are moving to default encryption that can only be decrypted by the customer). We then will move beyond the law enforcement context to consider, in Week 12, similar questions in relation to the activities of the U.S. Intelligence Community, including both espionage and covert action. And after that, in Week 13, we will elevate things still further by exploring the role of computer network operations during armed conflict.

10. November 1 – Should We Allow the Private Sector to Hack Back?

Are there circumstances in which we want someone in the private sector to be able to access another's system without their permission (and maybe without their knowledge)? We just completed a nine-week study of how the United States does or might discourage that sort of thing, so the idea at first blush seems jarring. But as we will see this week, there is a context in which some believe that the rules currently allow—or at least should be changed to allow—precisely this result.

The matter has been the subject of debate for years. Some call the idea "hackback," and some prefer the phrase "active defense." It's our focus this week.

<u>Why does this question arise? A hypothetical scenario to give us a frame of reference</u>

Assume an OPM-like scenario involving a private sector entity, which we will call Company X. The Chief Information Security Officer ("CISO") of Company X has just notified the CEO and the General Counsel that someone has gained unauthorized access to the company's network, has accessed sensitive files, has exfiltrated copies of some of these files to some external server already, and at this moment appears to be exploring for more such files.

You are the CEO. The CISO tells you that she has done some analysis, and is confident about a few things.

First, she has determined the IP address of the server where the attacker appears to have stored the exfiltrated files at least initially. She says that her team very likely could cook up some malware of their own in order to access that server, and once inside to locate and delete any of the company's files found there. It should also be possible to determine who controls the server, including the possibility that it is some innocent third-party whose own machine was compromised by the actual attacker in order to serve this staging function. In the latter case, the CISO says, it might also be possible to locate the server issuing orders to the compromised intermediate server, and so on until the identity of the attacker might become clear. The CISO is ready to make some or all of these attempts right now.

1. From a policy perspective, why might it be good to authorize the CISO to carry out some or all of these steps?

2. Why might it be bad?

3. Remember the Computer Fraud and Abuse Act. Do any of these proposed actions potentially violate the CFAA? Which specific section(s) of 18 USC 1030(a) might be violated?

4. If Company X cannot or should not take these steps, does that mean no one can? Which entities might become involved?

5. What downside is there, if any, if Company X stands down, leaving the task to that (those) entity(ies)?

Second, the CISO has identified the malware on the company's system that gave the attacker initial access to the company's system. Predictably, she says, it got there via an email phishing attack. You ask who was dumb enough to click on some infected link in an email. She coughs and looks at you uncomfortably, mumbling something about how this sort of thing could happen to anyone. You realize it was you… Happily, the CISO quickly changes the subject, explaining that she can easily remove the malware now.

6. Is it wise to take it out now? Why or why not? (Remember how OPM's leaders struggled with this question…)

7. Does this step present the same legal issue under the CFAA as in question 3 above?

The CISO says there is another option: She could lay a trap for the intruder, generating a file designed to be attractive to the attacker but loaded with a hidden beacon. A "beacon," in this context, is a program that will make periodic attempts to contact a control server in order to report on the current location of the file in which it is embedded. The CISO explain that this would be the digital equivalent of a GPS tracker hidden in a bag of cash stolen from a bank. She adds that she could even step things up a notch further, implanting code that would have a disruptive effect on the functioning of whichever system is hosting the file when it is opened.

8. Wise to take either step?

9. Legal?

<u>Going Deeper: A Look at the Hackback Debate Circa 2012</u>

You now have a frame of reference regarding the basic scenario that gives rise to the hackback debate, and that means you are in a good position to grapple in a more nuanced

way with the details of that debate. In 2012, Professor Orin Kerr and former NSA General Counsel Stewart Baker had an extensive and engaging online exchange on the topic. **Read the debate here** (this link compiles the full set of posts, which towards the end come to include Professor Eugene Volokh as well).

> *11. Baker's first post advances the policy argument for allowing some form of hackback. Why does he say a government response to an ongoing cyberattack on a private sector entity may be inadequate. What benefits does he say flow from allowing the victim to defend itself? How does he defend against the anticipated response that such victim self-help would be undesirable?*
>
> *12. Baker's second post argues not that the CFAA should be amended, but that even as currently written it should be construed not to apply to at least some hackback actions. What is his argument?*
>
> *13. Kerr responds on the legal side to claim that CFAA does currently apply, and that it would be bad were it otherwise. Can you summarize both those claims?*
>
> *14. Baker and Kerr go on to have an extensive back-and-forth on the CFAA interpretation issue. Who do you think wins?*
>
> *15. Kerr eventually introduces the idea that the better view is that the CFAA applies, but the victim company might avoid criminal and civil liability through the affirmative defense of necessity. Volokh adds that the victim also might prevail based on a defense-of-property theory. Is either the correct solution?*
>
> *16. Having studied this back and forth, go back to the Company X scenario above. Which if any of the actions suggested by your CISO would you be comfortable taking?*

Statutory Reform?

If you are inclined to think that certain forms of hack back may be desirable, but not actually allowed under CFAA (or, at least, not sufficiently clearly allowed), you might then consider (as Professor Kerr suggested in one of the posts above) the possibility of a statutory reform. And, indeed, some have pursued just that.

First, let's look back to a statute we previously studied in relation to information sharing. Remember CISA, the 2015 Cybersecurity Information Sharing Act? **Read Section 104(a),** copied below in full:

(a) AUTHORIZATION FOR MONITORING.—

1. IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—
   A. an information system of such private entity;
   B. an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

C. an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and (D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

2. CONSTRUCTION.—Nothing in this subsection shall be construed—

A. to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or

B. to limit otherwise lawful activity.

Consider how this statute might apply to each of the measures recommended by the CISO in the hypothetical case of Company X, above.

17. Does Section 104(a)(1) cover any of those measures?

18. Does Section 104(a)(1) make lawful anything that otherwise would be unlawful?

Next consider Section 104(b) of CISA, which speaks of certain activities that count as "defensive measures" as defined in CISA. Before looking at the text of 104(b), in fact, we should pause to look at the statute's definition of "defensive measures." Here it is, from Section 102(7):

7. DEFENSIVE MEASURE.—

A. IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

B. EXCLUSION.—The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

i. the private entity operating the measure; or

ii. another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

Now, on to Section 104(b) itself. It reads in full:

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

1. IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

A. an information system of such private entity in order to protect the rights or property of the private entity;

B. an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

C. an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

2. CONSTRUCTION.—Nothing in this subsection shall be construed—

A. to authorize the use of a defensive measure other than as provided in this subsection; or

B. to limit otherwise lawful activity.

Taking both Section 102(7) and 104(b) together, let's consider how they might apply to our hypothetical CISO suggestions:

19. Same questions as questions 17 and 18 above.

Not surprisingly, perhaps, CISA was not the last word on a possible statutory change relating to hackback. A few weeks ago, two members of Congress introduced a bipartisan bill called the Active Cyber Defense Certainty Act (that's right, it's the AC/DC Act; insert puns here!). **Read it here,** focusing on Sections 3 through 9.

20. For each individual section, be prepared to describe what it would accomplish, and whether this is a good or bad thing.

The bill has received a frosty reception in some quarters. Consider the commentary here.

21. Why would the FBI object?

22. Are there potential international relations complications? Try to imagine a worst case scenario.

23. Can you think of any creative ways to split the difference between what proponents of hacking back seek and the concerns opponents have raised?

11. November 8 - Law Enforcement & Network Investigative Techniques

Are there circumstances in which we want law enforcement officials to have the option of unauthorized access? More specifically, do we want there to be situations in which law enforcement by law has authority to circumvent the security of a machine or device without the owner/controller's knowledge or permission? And is this already possible to some extent under current law and policy?

There are many variables to consider under this heading. Is the system to be breached in America or elsewhere? How will the breach be effectuated? Will it have effects other than acquisition of information? Does it run the risk of diplomatic repercussions, and if so of what likely kind and severity? Who will decide whether to do it, who will actually do it, and what oversight if any might there be? And would it be legal?

Read this article from Kim Zetter at Wired for an overview of this question, focused on the FBI.

1. Consider a high-altitude question of policy first: What are the benefits of allowing law enforcement to take such steps, and what costs?

2. To obtain a search warrant, the government must have enough evidence to persuade a federal judge that there is probable cause to believe a crime is or has been committed. The showing is made in private and without opposing counsel, for the obvious reason that to do otherwise would be to tip off the target of the impending search. In the event of a subsequent prosecution, the defense may retroactively challenge the warrant by moving to suppress evidence obtained under it. Does this process satisfy any concerns you might otherwise have in relation to Network Investigative Techniques (NITs)?

3. Would any of your answer differ if we are speaking of a state or local law enforcement entity rather than the FBI?

4. The article notes that FBI obtains search warrants authorizing the use of such methods in some cases but not all. Why is that? Hint: Think about geography.

5. What are the international relations implications of NITs employed to access systems located elsewhere?

6. The first example in the article is "Carnivore." That system was more in the nature of a wiretap than a technical hack to circumvent information security measures. But it is a useful setup to explain the government's interest in "keylogger" software. What is a "keylogger" and what technical problem does it solve?

7. The Scarfo investigation led to a complaint by a Justice Department official suggesting that FBI had "risked a classified technique on an unworth[y] target." What harm could follow from using the keylogger at issue there?

8. What was different about Magic Lantern as compared to the Scarfo keylogger?

9. The next example—CIPAV—concludes with the notion that Justice Department officials worried that excessive use of the NIT increased the "risk of suppression." Does that mean something improper was going on? What could CIPAV do and when is that desirable?

10. The Watering Hole Strategy: What is a "watering hole" in this context, and why might this approach be useful for NIT delivery?

11. Ponder what steps the government must go through in order to effectuate a watering hole/NIT strategy. Anything stand out as particularly tricky or difficult?

12. The piece concludes with "Big Questions Remain." Read carefully, and decide which of these questions seem most significant to you.

As questions 4 and 5 above noted, sometimes NITs target systems that are located overseas and thus give rise to serious international relations and legal complications. **Read this short paper from Orin Kerr and Sean Murphy** exploring some of the resulting issues.

13. What did Professor Ghappour argue regarding the implications of international NITs for international relations, how did Kerr and Murphy respond?

14. Why might one think that an international NIT violates international law, and why do Kerr and Murphy reject that view?

15. What if anything do we learn here regarding the internal system of management and oversight regarding the use of international NITs?

Let's set aside those international complications for a moment, and focus on what happens when the fruits of an NIT are used to prosecute. As we saw above, the Justice Department and FBI worry about maintaining the secrecy of how some such tools work. **Read this Lawfare piece by Susan Hennessey and Nicholas Weaver** in order to better understand how NITs function and why prosecutions can result in dilemmas pitting the interests of preserving secrecy against those of securing convictions.

The Lawfare piece notes the connection between the idea of law enforcement hacking and the government's oft-stated fear that the diffusion of strong encryption can and will produced a "going dark" situation in which the government has a warrant (or other lawful authority) to access a system (a laptop, a phone, a message in transit) but neither it nor the company that made the system can decrypt the information therein. **Read pages 1-15** (as numbered in the original text of the document, not just counting from the start of the pdf) **of the "Don't Panic" report** issued by the Berkman Center at Harvard. **Then read this essay from Susan Hennessey for Brookings** (titled "Lawful hacking and the case for a strategic approach to 'Going Dark'").

16. What are the policy concerns that motivate the FBI here?

17. What are the offsetting policy concerns?

18. What factors might make the situation worse for the FBI over time, and what factors might make it better?

19. What role does the "lawful hacking" idea play in addressing "going dark," and is it necessarily cost-free to encourage resort to that solution?

20. Are state/local law enforcement entities similarly-situated to the FBI with respect to these debates?

12. November 15 - Espionage and Covert Action

This week, we'll look at "authorized unauthorized access" (*i.e.*, access that is legally-authorized from a U.S. perspective but that does not involve the permission (and usually not the awareness either) of the owner/operator of the system in question) where the "attacker" is a U.S. government entity engaging in an "intelligence activity."

What Do We Mean By "Intelligence Activity"?

Let's be clear about what we mean by "intelligence activity." This phrase means different things to different people, but for our purposes it will suffice to say that there are three areas of activity that can fall under that heading:

1. Analysis

This refers to the process in which experts employed by an intelligence agency pour over various sources of information and convey the resulting knowledge to government "customers" (such as the President) in the form of intelligence "products" (such as the President's Daily Brief). Analysis, in short, is a form of scholarly activity intended to inform government decisionmakers.

2. Collection (Espionage)

Collection is the process of acquiring information or data in the first place, in order that it might be used for analysis. Collectors may gather information from open sources the same as anyone else, of course, but the distinctive feature of collection performed by an intelligence agency is *espionage—i.e.,* stealing secrets. This can occur through recruitment of human sources, through wiretapping of electronic communications, through physical break-ins, through hacking, and so on.

3. Covert Action

Covert action is a legal term-of-art describing any activity in which the government seeks to cause an effect but without the sponsoring role of the U.S. government being apparent or acknowledged. Covert action can run the gamut of intensity from minor efforts to influence political opinions in a foreign state to the use of lethal force (*e.g.,* the much-publicized CIA drone strike program that has operated in Pakistan and elsewhere in the post-9/11 period).

While these three activities are conceptually distinct, real-world fact patterns do not always fall neatly into just one category. Consider this example: A CIA officer forms a strong relationship with an Iranian scientist involved in Iran's nuclear program. The scientist is willing to share secrets, to cause problems for the nuclear program by interfering with equipment, or both. Should we categorize the recruitment as collection or covert action? The answer depends on the state of affairs at a given moment in time.

1. Can you explain how the same thing is true with respect to an intelligence activity in which an agency uses an exploit to gain undetected access to a computer belonging to a foreign government?

An Introduction to the U.S. Intelligence Community ("IC")

Some of you may already be familiar with the various agencies that collectively constitute the U.S. government's "Intelligence Community" (a.k.a., the "IC"). I will assume the topic is new to all of you, however. What follows is a thumbnail sketch of the IC.

The IC consists of *sixteen* different entities, plus an additional entity—the Office of the Director of National Intelligence (ODNI), which is led by the Director of National Intelligence (DNI)—which is designed to play an overarching coordination role. You might think that the sixteen entities thus all report to the DNI and no one else. That's not how it works, though. Most of the sixteen entities are part of a separate department of government (many of them are part of the Defense Department, while others are part of the Justice Department, the Department of Homeland Security, the Energy Department, the Treasury Department, and the State Department). And then there is the fiercely-independent CIA.

Which entities perform which functions? We will touch on only a few key points that happen to relate in particular to cybersecurity.

1. The National Security Agency ("NSA")

NSA is part of the Department of Defense, and has a complex set of missions. Most obviously, it is the lead agency for collecting foreign intelligence through electronic means in order to suit the needs of national customers like the President. Less obviously, it also collects to address the needs of military customers, including collection in support of ongoing combat operations. Further, NSA has a parallel defensive mission (as we have noted previously when discussing the protection of government networks). NSA also performs analysis of the information it collects.

2. The Central Intelligence Agency ("CIA")

CIA is an independent federal agency that performs all three intelligence activities described above. It is the premier agency for conducting collection through human sources, though its collection methods are not limited to that approach. CIA also is the premier agency for conducting covert action.

3. The Federal Bureau of Investigation ("FBI")

The FBI is, first and foremost, a law enforcement agency. But it also performs collection and analysis with respect to foreign intelligence matters arising inside the United States.

2. Can you state, and explain the differences among, NSA's three major missions?

The Domestic Legal Framework for Collection and Covert Action

Over the past five decades, the United States has developed a complex legal framework relating to both collection and covert action activities. A full study of that framework is beyond the scope of this course (my Law of the Intelligence Community course covers it). There are some highlights that we should address, however.

The legal framework addresses three types of question:

1. Authority

What is the affirmative legal authority for various agencies to conduct intelligence activities in the first place?

Let's consider collection first. There is little real debate regarding the general authority of the President, under Article II of the Constitution of the United States, to collect foreign intelligence information. And various statutes and executive orders in turn have tasked particular parts of the executive branch—notably, NSA and CIA—to carry out this function.

Covert action once was different. That is, there used to be a significant debate regarding whether the CIA in particular really had statutory authorization to engage in such unacknowledged activity. Beginning in the early 1970s, however, Congress began imposing process rules relating to covert action decisions and oversight(see the next section below). As that framework grew, it became increasingly untenable to question whether CIA was authorized to engage in covert action in the first place.

2. Process

(a) Ex ante approval: The first process question to consider is whether any particular procedures must be followed *before* deciding conduct either collection or covert action.

Collection*:* The interesting "process" question with respect to collection is whether and when the government must obtain *judicial* approval to engage in a particular collection activity. This is an immensely complex topic, covered in detail in my Law of the Intelligence Community course. For our purposes, we will just scratch the surface.

Let's begin with the Fourth Amendment to the Constitution of the United States. It requires that all "searches" be "reasonable," and provides that no warrant shall issue from a court except upon a showing by the government that it has sufficient evidence to establish "probable cause" to believe that a crime has been or is being committed, and that the search of a particular location will discover particular evidence of or fruits from that crime. At first blush, that might seem to require the government to go to court to obtain particularized warrants before engaging in collection activity, including collection via unauthorized access to a computer system. Not all government information-gathering activity triggers the Fourth Amendment, however.

There are several complications. First, the Fourth Amendment does not apply to non-US persons outside the United States. Second, some courts have held that the Fourth Amendment does not apply to government information gathering conducted solely for foreign intelligence purposes (as distinct from law enforcement purposes), though the Supreme Court has never delivered a holding on this question one way or the other. And third, Congress in 1978 crafted a statute that to a substantial extent makes the Fourth Amendment question moot, by imposing a warrant-like requirement in the cases most likely to raise the Fourth Amendment issue: The Foreign Intelligence Surveillance Act of 1978 ("FISA" (pronounced fie-suh, not fih-suh)).

FISA is a complex statute, and we are not going to try to study it to a serious degree. But you do need to have a rough sense of what it requires and when that requirement attaches. Simplifying things quite a bit, we can boil it down to the following. FISA requires the government to make a probable cause showing that the target of its

collection is an agent of a foreign power in order to collect the content of electronic communications, but only in specific scenarios. Specifically, this obligation attaches in situations with strong Fourth Amendment equities: where the target is a U.S. person inside the United States, or where the communication has at least one end in the United States and the collection will take place in the United States.

There are many further complications with surveillance law, but they are beyond the scope of our course. For now, it suffices to understand that collection of the content of electronic communications sometimes requires application to a court, and sometimes not.

> *3. Can you explain why the Fourth Amendment does not clearly require a court-issued warrant for all collection activities, period?*
>
> *4. What are the benefits of judicial involvement in deciding to collect?*
>
> *5. What are the costs of such involvement?*

Covert action: There is a simpler framework that governs the decision to engage in covert action, and it does not concern courts. Instead, it is a matter of requiring particular executive branch officials to sign-off on covert action proposals. Title 50 of the US Code requires that any activity counting as a covert action must be approved by the President in writing. We call that the requirement of a presidential "finding." This has been the rule since the early 1970s. Prior to that time, there were no statutes attempting to regulate the covert action decision-making process, and presidents were under no obligation to commit in writing to the approval of covert action programs.

> *4. Give thought to the incentives the Title 50 finding requirement creates. If you were President, what sort of internal executive branch process might you want to have in place in order to ensure you make good decisions on signing findings?*
>
> *5. Not all or even most covert action involves hacking. But sometimes it will. Does your answer to question 4 change in any way for such cases?*

Note: Title 50's definition of covert action includes an express exemption for any otherwise-qualifying activity that counts as a "traditional military activity" (a.k.a. "TMA"). That makes the definition of TMA rather significant, since the requirement of a presidential finding drops out when it applies; an operation that qualifies as TMA therefore is not a "Title 50 activity" after all, but instead a "Title 10 activity" (Title 10 being the part of the U.S. Code that addresses the Defense Department).

Alas, there is a long history of confusion surrounding the definition of TMA (and, hence, a long history of confusion about the line between Title 10 and Title 50 operations). Simplifying things a bit, there are two camps. One takes a literal approach, emphasizing whether the activity in question is being conducted by the military and whether it is the sort of thing that historically has been done by the military in particular. The other camp focuses (more accurately, in my view) on the detailed legislative history of the TMA statutory exemption. That legislative history makes clear that Congress did not intend to make historical military practice as such the central question. The issue, rather, is whether the operation in question is to be commanded and conducted by military personnel, and whether it relates either to an ongoing armed conflict or to a circumstance for which operational military planning has taken place (which is a *very* wide set of circumstances).

*6. **Read this article about the "Stuxnet" episode.** Would you characterize this as covert action or TMA? Consider that question separately in light of the two distinct understandings of TMA mentioned above.*

2(b) *Ex post* reporting: Regardless of whether a statute requires any particular ex ante decisionmaking procedures, there is a question regarding whether the executive branch has to report to Congress regarding its intelligence activities. The answer this time is yes as to both collection and covert action. Both the Senate and the House each have a standing committee to receive these notifications: the Senate Select Committee on Intelligence (SSCI (pronounced sis-see) and the House Permanent Select Committee on Intelligence (HPSCI (pronounced **hip**-see)). For covert action, Title 50 requires notification to special Congressional committees of the presidential findings mentioned above. For collection, Title 50 requires those same committees to receive notification.

7. What values does this arrangement serve?

8. Why not simply require all of these matters to be made public?

3. Substantive legal limits: In theory, Congress could specify certain things that NSA, CIA, and other intelligence agencies simply may not do when collecting or engaging in covert action. For example, it could ban certain more extreme forms of covert action. Or it could impose geographic constraints. And so forth. So, what has Congress actually done?

3(a) Collection – There is a vast and complex set of legal rules

3(b) Covert action - There are a few substantive rules set forth in 50 U.S.C. 3093. First, section 3093**(f)** provides that covert action cannot be used with intent "to influence United States political processes, public opinion, policies, or media."

8. Consider the following hypothetical situation: A president wants CIA to conduct a covert action that would include efforts to hack the personal email and social media accounts of various prominent foreign officials, then use the information obtained to plant stories in that country's media in hopes of impacting an upcoming election. Would this be barred by section 3093(f)?

Another part of Section 3093—3093**(a)(5)**—states that the president's finding authorizing a covert action "may not authorize any action that would violate the Constitution or any statute of the United States."

9.Refer back to the hypothetical situation in the previous question. Would section 3093(a)(5) prohibit that activity?

10. The proposed activity certainly would violate the criminal laws of the foreign state in question. Setting aside all other considerations, does this matter from a U.S. domestic law perspective? That is, does it follow from this that American law also forbids such an action?

11. As we will discuss in more detail below, the proposed activity might also violate international law. Setting aside all other considerations, does this matter from a U.S. domestic law perspective? That is, does it follow from this that American law also forbids such an action?

12. Change the hypothetical such that a US agency will hack into foreign systems to acquire information, but nothing else will occur except the use of this information for analysis purposes. Reconsider questions 9-11 in this light.

13. Change the hypothetical again, such that a US agency will hack into a foreign system for purposes to be determined later as circumstances dictate. What complication does this introduce, and does it alter any of your answers?

International Law & International Relations

What *does* international law have to say about the use of cyber means to conduct espionage or covert action, anyway, and why does this matter? We will start with the latter question.

14. Create a list of factors why the U.S. government might or might not care about the international legality of espionage and covert action involving cyber methods, as contrasted with reasons it might or might not care about their legality under US law.

15. If your list contains any factors involving potential diplomatic (or other non-legal) repercussions, consider whether and to what extent the risk of those repercussions actually depends on a good-faith belief by the impacted state that the United States actually violated international law.

16. In the preceding section we noted that U.S. law arguably gives a green light to some agencies to act contrary to international law when conducting covert action. Go through your list of cautionary factors, and note any of them that would be negated or at least substantially reduced by such a domestic law provision.

Now, let's assume that international law does indeed matter (at least to some extent). What does it have to say about espionage and covert action in general, and as applied to cyber methods in particular? This is a contested topic, to put it mildly, but the following summary observations will give us a good orientation.

1. Use of Force?

Though we will not talk in detail about the cyber aspect of armed conflict until next week, we nonetheless should start with Article 2(4) of the U.N. Charter. It creates a default rule prohibiting the "use of force" in international affairs. To be lawful, a use of force on the territory of another state requires that state's consent; an affirmative authorization from the U.N. Security Council; or a situation in which the state is using force in individual or collective self-defense in response to an "armed attack." The U.S. government also takes the position that a state can effectively waive its objection to the use of force if that force is a necessary and proportional response needed to suppress armed attacks emanating from a non-state actor within the other state's territory, if the host state proves unable or unwilling to address that threat.

17. Most cyberspace activities would not seem to trigger a discussion of these rules. But some might. Describe factors that you think should be relevant.

2. Internationally Wrongful Acts & the Law of "Countermeasures"

Just because an action falls shy of a "use of force" does not mean that international law has nothing to say about it. The question then becomes: is the action instead an internationally wrongful act? If so, this may entitle the aggrieved state to take a "countermeasure."

To understand these concepts better, let's refer to the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." The Tallinn Manual is not itself a legal instrument, though it is written in terms of "rules." It is a scholarly product, resulting from a multi-year set of discussions among a large group of international law experts from a variety of countries (conducted under the auspices of the NATO Cooperative Cyber Defense Center of Excellence, but not constituting the views of NATO or any particular state as such). It is framed as a summary of current law accompanied by commentaries (though some critics contend that some of the rules it identifies are more aspirational than descriptive of existing law). It is, at any rate, a convenient source to frame our discussion.

Rule 20 of the manual provides that a "State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State." Put more directly: if one state acts illegally towards another, it opens up the door to the victim retaliating with methods that otherwise would violate international law.

Countermeasures are not punitive as such. Rather, they must be intended to induce the offending state to stop violating international law. (Rule 21) They are not an anything-goes situation, either. They may not "affect fundamental human rights," for example. (Rule 22) And they "must be proportionate to the injury to which they respond." (Rule 23) They need not involve the same means or domain that produced the original injury, however; they can be cross-domain in nature. (Rule 24)

> *18. Assume that Russian intelligence agencies are engaged in a covert action program to impact elections in the United States. Identify a "countermeasure" the United States might then employ that (i) complies with the aforementioned rules yet (ii) actually might help remedy the situation.*
>
> *19. Same situation, but the election is question is now over. Analysts advise that there is plenty of reason to assume the same thing will occur during the next election cycle, but there is no specific intelligence confirming this. Is it still proper to engage in a countermeasure?*

Countermeasures by definition come into play only where the other state has engaged in a wrongful act (or where that state is responsible for the wrongful acts of private individuals/entities who did so). This raises the question of when a cyber activity might cross the line.

> ***Collection:*** Rule 32 of the Tallinn Manual 2.0 generally accepts the international legality of espionage, including cyber espionage, but with caveats. The experts involved in drafting it "agreed that customary international law does not prohibit espionage *per se*." (Rule 32 note 5) By extension, they concluded, "peacetime cyber espionage by States does not *per se* violate international law." (Rule 32) (emphasis added). That said, "the method by which it is carried out might do so" in a particular case. (Rule 32). For example, the experts suggested, a violation of sovereignty would occur if a state engages in cyber espionage "in a manner that results in a loss of functionality" to "cyber infrastructure located in another State." (Rule 32 n.6). The experts also raised the possibility that cyber espionage might clash with an asserted (but contested) international human right to privacy (*id.*). The experts apparently disagreed on an array of more specific matters, such as whether the significance of the information stolen via cyber espionage might at some point render the espionage a violation of sovereignty after all. (Rule 32 note 8). Note, too, that the experts concluded that unintended consequences from cyber espionage—such as disruption of the functioning of the penetrated system—could render the activity unlawful. (Rule 32 no. 14).
>
> *20. Do you agree with these characterizations of collection activity conducted via cyber means?*

Covert Action: As noted above, covert action programs can run the gamut from minor matters to actions constituting armed attack and the use of force. Covert action through cyber means similarly can vary in terms of its nature and intensity, complicating any attempt to describe the legality of this category as a whole. Against that backdrop, the Tallinn Manual identifies both a general principle of protecting sovereignty, and a more specific rule against "intervention" in sovereign affairs. Let's focus on the latter.

Rule 66 of the Tallinn Manual 2.0 provides that a "State may not intervene, including by cyber means, in the internal or external affairs of another State." The notes to Rule 66 explain that the rule derives from the principle of the sovereign equality of states. But when exactly does a cyber operation constitute a prohibited intervention? The experts emphasize that there must be an element of coercion (n. 6), though that term "is not defined in international law" (n.18). The experts offer this definition: "an affirmative act designed to deprive another State of its freedom of choice…to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way" (n.18). The experts offer several examples, including (i) "using cyber operations to remotely alter electronic ballots and thereby manipulate an election" (n. 2), and (ii) conducting a DDoS attack on State B in order to induce it to withdraw recognition of State C (n. 20).

Now, a further wrinkle: Rule 26 provides that a "State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."

21. Assume that the United States and Israel team up to create malware that will cause centrifuges at an Iranian nuclear facility to spin out of control, resulting in substantial physical damage (but not likely the loss of life). Does this constitute a forbidden intervention? Might it even be a use-of-force? Or does the "plea of necessity" apply?

22. Same situation: If you are asked by the President to advise whether to undertake such an operation, what considerations might you bring to bear apart from the international law questions?

What about international "norms" (as distinct from international "law")?

Read **this article** on the surge of interest, circa 2015, in developing less-formal forms of international agreement about proper behavior in cyberspace (including but not limited to the US-China agreement on limiting cyberespionage conducted to benefit commercial enterprises).

23. Can you explain what a "norm" is and how it differs from "law"?

24. Can you explain how a "norm" might smooth the way towards later claims about "law"?

25. If you worked for the Russian or Chinese governments, would you find the "norms" model attractive?

26. Should the U.S. government embrace the norms model?

NOTE: NO CLASS ON NOVEMBER 22 (THE DAY BEFORE THANKSGIVING)

13. November 29 - Armed Conflict and Cyberspace

(Reminder: During class #12, we did not reach the Week 12 materials on (i) the substantive "red lines" in American domestic law that limit covert action and (ii) the international law concepts implicated by both espionage and covert action. Our class for Week 13 therefore will pick up with those topics, before turning to the (closely-related) new material for this week. Now, on to the new readings for Week 13…)

Last week we examined how the U.S. government's Intelligence Community (including but not limited to NSA) engages in "authorized unauthorized access" for purposes of espionage and covert action. This week, our focus switches to the cyberspace activities of the U.S. military.

At the risk of oversimplifying things, we might say that the military engages in three types of activity in this context. First, it collects information. Rather than calling that espionage, the military traditionally describes information collection as "ISR," meaning "Intelligence, Surveillance, and Reconnaissance." Second, the military engages in activity to defend its own networks. Those networks are known, collectively, as the Department of Defense Information Network, or "DODIN" (one commentator has described DODIN as "really not a single network, but a quasi-feudal patchwork of often incompatible local networks[;] It's the Holy Roman Empire of cyberspace"). Third, the military conducts cyber operations to cause effects, such as disruption or alteration of enemy communications.

We are concerned primarily with this third, operational, type of activity. We'll focus on six aspects of that topic:

1. Terminology
2. Institutions
3. International law rules
4. Domestic law rules

1. Terminology

We start with an overview of the relevant terminology, bearing in mind that there can be a significant difference between common usage of a term and that same term's peculiar legal meaning.

The words "war" and "warfare" are good examples. They are used frequently by policymakers, legislators, journalists, pundits, and just about everyone else. Most would agree they cover at least the paradigm case of violent engagement between military forces, but beyond that one finds varying degrees of disagreement regarding which other situations of violence might also warrant those labels. Add to this the temptation to use phrases like "cyberwarfare" relatively promiscuously, and one has a recipe for confusion even without factoring in the possibility that the relevant *legal* categories don't use these terms at all.

1. Spend a few minutes searching online using Google News (or the like) for recent uses of "cyberwarfare" or "cyber warfare." Does it seem to you that "war" is being overused in this context? Or might it be that activities in cyberspace warrant a broader conception of "war" than one might use in physical space?

However important and common the word "war" is in relation to policy, politics, and diplomacy, the fact remains that it no longer plays a dominant role in relation to the legal frameworks we use to regulate military activity. As described in more detail below, the most important international law questions today turn on whether one should categorize a situation as "armed conflict," a "use of force," or an "armed attack," and the most important domestic law questions focus on concepts such as "hostilities."

"Attack" presents a similar issue. That word is used routinely to describe hostile cyber activities without the user meaning to suggest a particular legal characterization, yet the word does have specific legal meaning. Again, the difference can result in some degree of confusion or cross-talk.

2. Do another search, this time looking for uses of the words "cyberattack" or "cyber attack." Do the examples all concern activities analogous to a physical-world military attack?

3. Set aside whether these words have special legal meanings. Considered just from the perspectives of policy, politics, and diplomacy—or just journalism itself—does it matter if the terms are used loosely? And is there any realistic alternative?

2. Institutions

Our next task is to become acquainted with the institutional structures the U.S. military has adopted in order to facilitate its activities in cyberspace. As you might expect, there has been a great deal of organizational change in recent years, and more is likely to come in the near future. We will not attempt anything close to a comprehensive overview, but we will at least identify some of the most important current institutions and some of the bigger issues that they face.

As an initial matter, let's recall that the NSA itself is part of the Defense Department, and that one of its core missions involves collection for combat-support purposes. And we should note, as well, that a Defense Department entity known as the Defense Information Systems Agency ("DISA") performs certain defensive functions as part of its core mission to support the Department (including combat operations) with IT and communications services. But all this leaves open the question of how the Defense Department organizes the armed services themselves for purposes of conducting cyberspace operations in combat and other settings.

As Fred Kaplan explains in his recent book *Dark Territory: The Secret History of Cyber War*, the effort to organize for offensive cyber operations traces back to the late 1990s. As the Department began to appreciate how vulnerable its own networks were, it established a new office—the "Joint Task Force—Computer Network Defense," or just "JTF-CND"—to coordinate defensive efforts. Kaplan writes that the

> "initial plan was to give [JTF-CND] an *offensive* role as well, a mandate to develop options for attacking an adversary's network.… [But the organizer] knew that the services wouldn't grant such powers to a small bureau with no command authority. … [Eventually, in] 2000, JTF-CND became JTF-CNO, the *O* standing for "Operations," and those operations included not just Computer Network Defense but also, explicitly, Computer Network *Attack*.… [JTF-CNO] was placed under the purview of U.S. Space Command…it was an odd place to be, but SpaceCom was the only unit that wanted the mission…[and] in any case, it was a *command*, invested with war-planning and war-fighting powers. [But key leaders] felt that the cyber missions—especially those dealing with cyber *offense*—should ultimately be brought to the Fort Meade headquarters of the NSA." (pp. 121-22)

It took many years, but that is exactly what happened in the end. In the summer of 2009, Secretary of Defense Gates directed the creation of a new command—United States Cyber Command (CYBERCOM)—focused on these defensive and offensive functions. It would be collocated with NSA at Ft. Meade, and NSA's Director would be "dual-hatted" as the CYBERCOM commander as well.

So, what exactly does CYBERCOM do? The Defense Department's 2015 Cyber Strategy document provides a handy explanation:

> *"In 2012, DoD began to build a [Cyber Mission Force ("CMF")] to carry out DoD's cyber missions. Once fully operational, the CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components…. The Cyber Mission Force will be comprised of cyber operators organized into 133 teams, primarily aligned as follows:*
>
> > ***Cyber Protection Forces*** *will augment traditional defensive measures and defend priority DoD networks and systems against priority threats;*
> >
> > ***National Mission Forces*** *and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence; and*
> >
> > ***Combat Mission Forces*** *and their associated support teams will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations.*
>
> *Combatant commands integrate Combat Mission Forces and Cyber Protection Teams into plans and operations and employ them in cyberspace, while the National Mission Force operates under the Commander of USCYBERCOM. Outside of this construct, teams can also be used to support other missions as required by the Department."*

Note the separate reference there to "combatant commands" (which will employ the Combat Mission Forces and the Cyber Protection Forces) and CYBERCOM (which will employ National Mission Forces). This calls for a quick primer on what a "combatant command" is.

The traditional organizational structure of the Armed Forces of the United States involved a division into a series of separate "service branches": the Army, Navy, Air Force, and Marines (and the Coast Guard as well, though its precise status is complicated). These branches both trained

and equipped their own forces, and also conducted operations—often (though not always) in coordination with one another. Eventually, however, this model gave way to a more-integrated approach. Today, the separate branches remain in charge of recruiting, training, and equipping servicemembers in the first instance, but we now have a "joint forces" model for purposes of actual operations. Under this model, assets from each branch are controlled for operational purposes by a single command structure (as opposed to having, say, separate and equal Army and Navy commanders operating in the same location). More specifically, we now have a globe-spanning series of *geographically*-defined "combatant commands," such as Central Command (CENTCOM, which encompasses the Middle East through to Afghanistan) and Pacific Command (PACOM).

So far so good, but it gets more complicated. In addition to these geographically-defined commands, we also have several additional commands that have no geographic boundaries but instead are defined by the particular function they perform or support. CYBERCOM is such a command. Special Operations Command (SOCOM) is another. These functional commands are like the geographic ones in that their subordinate units and personnel all hail from one of the various service branches, brought together under a "joint" command structure for operational purposes. In CYBERCOM's case, that means that Army, Navy, Air Force, and Marine cyber units and personnel actually make up the various Cyber Mission Forces.

Against that backdrop, it is easier to understand the description of CYBERCOM's dual role. First, CYBERCOM is charged with ensuring that the geographic combatant commands like CENTCOM are supported with Combat Mission Forces and Cyber Protection Teams. One might think that this support function could simply be met by the service branches separately and directly, but given the specialized expertise and technologies involved it is not hard to see why the centralized approach via CYBERCOM makes more sense. Second, CYBERCOM has its own operational responsibility, to be executed via the National Mission Forces (which answer to it, rather than to any geographically-defined command).

So, how far along is CYBERCOM as of late 2017? The Army and Navy recently announced that they have completed training their share of the Cyber Mission Force teams (covering about 60% of the total). Air Force and Marine units have until late 2018 to complete the training of the remaining teams.

A final issue worth emphasizing: As CYBERCOM reaches maturity, the need for it to be commanded by the same person who serves as NSA Director to some extent diminishes, insofar as the point of having the same person command both entities serves to ensure that CYBERCOM can get the benefit of NSA's extraordinary expertise, technology, and personnel. There is widespread agreement that the "dual hat" arrangement therefore should end at some point (including legislation and presidential orders to that effect). But everyone also agrees that care must be taken before actually making that move, and it remains unclear when it actually will occur. Complicating matters further, the "dual-hat" question may implicate significant issues beyond questions of operational competence and expense. **Read this post from me, on Lawfare,** providing the history of what we might call the intelligence-operational deconfliction question.

> *4. Can you explain how collection equities might clash with the military's operational interests?*

5. How does the dual-hat arrangement help address that clash, and what would likely happen instead if CYBERCOM and NSA are separated at the command level?

Note that the deconfliction challenge is not necessarily a matter of a clash between the Intelligence Community and the military, as such. Other competing equities, such as diplomatic or legal considerations, also might come into play with a proposed military cyber operation, thus calling for a structure that would sensibly balance the benefits of conducting that operation against competing costs or constraints that might not be within the lane of a military commander in the field. From that perspective, consider this report of a recent speech from CENTCOM's commander, General Votel, addressing cyber operations against the Islamic State:

> *"We at [Central Command] have narrowly defined authorities to execute cyberspace operations at all, let alone execute the required initiative and adaptive thinking towards countering this pervasive threat," Votel said.*
>
> *At one level, that makes sense, he said. "For very good reasons and concerns about cyberspace operations propagating outside the intended joint operation area, a lot of the approval authorities to execute these types of operations reside with the president or the Secretary of Defense."*
>
> *Those reasons include the need to have someone in charge of strategy coordinate various combatant commanders. But, Votel continued, "at the operational level, the level at which cyberspace operations are integrated with conventional and special operations forces, this can make approval so cumbersome that the capabilities are nearly irrelevant."*

[The quoted passage is from this article by Patrick Tucker. Feel free to read the whole piece if you are curious, but you are not assigned to do so.]

6. What sort of computer network operations might General Votel have in mind?

7. Can you explain the competing equities that have led to approval authority being held back to the Secretary of Defense or Presidential levels?

8. Should something change to address General Votel's concerns? Give thought to what alternative problems might arise if authority to conduct operations is pushed out to commanders in the field to a much greater extent.

3. International law rules

Now that we have a sense of which parts of the U.S. military might engage in cyber operations, it is time to review the legal architecture governing that activity. We'll start with the international law framework, before turning to the U.S. legal framework.

Last week's readings introduced the U.N. Charter and its default rule (under Article 2(4)) against the "use of force" in international affairs. This raises the question: When does a computer network operation count as a "use of force," if ever? The Tallinn Manual 2.0 offers the following interpretation:

> **Rule 69 "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."**

9. Imagine that CYBERCOM manages to hack into a Russian military communications system, and steals data from it. Is that a "use of force"?

10. Same issue, but this time CYBERCOM causes the system to stop functioning for one hour.

11. Same, but this time CYBERCOM causes the system to overheat, resulting in physical damage that ruins the system.

12. Same, but this time CYBERCOM causes the system to explode, killing several nearby personnel.

13. Assume that the correct answer at some point becomes yes. What exactly follows from this? Does it mean America and Russia are in a "war"? Does it mean Russia necessarily will respond in a particular way?

As noted last week as well, one of the exceptions to Article 2(4)'s prohibition on the "use of force" is a situation in which a state's right to use force in self-defense has been triggered by an "armed attack." This is stated in Article 51 of the Charter, which recognizes self-defense both on an individual and a collective basis (the latter meaning that one state may ask another to come to its aid if the former has been attacked). Thus the question arises: does "armed attack" mean anything different from "use of force"? The Manual argues that "all armed attacks are uses of force," but some actions short of "armed attack" might still count as a "use of force." (p.333)

A final consideration before moving on: Does the law of armed conflict apply to computer network operations? That is, are they subject to the familiar law of armed conflict rule such as the prohibition on intentionally attacking civilians and civilian objects (a rule that has exceptions, of course, such as the exception for civilians who are in the midst of participating in hostilities, or civilian objects being used for military purposes), and the "collateral damage" rule that forbids attacks on otherwise-permissible targets where the anticipated civilian harm will outweigh the expected military benefit. The Manual explains:

Rule 80: "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict."

14. Read that closely. Does it mean that <u>all</u> computer network operations conducted by a military entity are subject to the law of armed conflict at all times? Conversely, does it mean that computer network operations conducted by a non-military unit are not so subject?

4. <u>Domestic law rules</u>

We will consider two issues: (i) affirmative authority to act in the first place, and (ii) oversight rules.

First, from where does the authority to conduct a military cyber operation derive in the first place?

This question, from a legal perspective, is much the same as would be true for a non-cyber activity conducted by the U.S. military. We can spend an entire course exploring the

controversies that attend this topic, but our aim is not to master this topic. Rather, we just need to understand the basics of the debate, and where cyber operations fit into that picture.

As an initial matter, the President has inherent authority under Article II of the Constitution to direct the use of the military to defend the United States in case of attack. Outside the context of self-defense, however, things get complicated. Some take the view that all uses of military force in such cases must be supported by affirmative authorization from Congress, such as a Declaration of War or an express "Authorization for Use of Military Force" ("AUMF") along the lines of the 2001 AUMF authorizing force against al Qaeda and the Taliban. Others take the view that the course of practice over time has empowered the President to use force on his own initiative at least below the threshold of full-scale armed conflict with American soldiers on the ground. And others take intermediate positions, such as requiring Congressional approval but finding such approval in less-direct sources, such as funding bills.

Bearing that in mind, consider the following solely in relation to the question of affirmative domestic legal authority:

> *15. The United States for many years has conducted high-intensity military operations against the Islamic State in Iraq and Syria, primarily relying on the 2001 Authorization for Use of Military Force against al Qaeda (on the theory that IS is the direct descendent of al Qaeda in Iraq). Does a CENTCOM cyber operation to take down an IS website require an additional authorization apart from that? Does the geographic location of the server in question factor into your analysis?*
>
> *16. Assume that the President directs the military to carry out an operation to hack into a North Korean government server, and delete all the data there. Assume the operation is not a covert action. Can you make an argument that there is not sufficient legal authority to do this? Can you make a contrary argument?*

Second, let's consider the question of oversight.

With covert action, as we saw last week, U.S. law requires both a presidential finding on the front end and a notification of that finding to key Congressional committees on the back end. The question we now want to consider is whether there is anything similar for the military's computer network operations.

For most military activity in a non-cyber setting, a general form of oversight ordinarily occurs through the regular exchange of information between the Pentagon and the Senate and House Armed Services Committees. If and when U.S. forces are deployed into hostilities or into situations in which hostilities are imminent, moreover, a statute known as the War Powers Resolution requires a formal notice to Congress within 48 hours. Apart from this, however, there historically was not a more-granular notification process akin to the covert action oversight system.

In recent years, this began to change with respect to "kill/capture" operations that might be conducted outside of conventional war zones. The idea was that such operations are especially sensitive, and thus an operation-specific notification system (with notification given to the two Armed Services Committees) might be desirable. At the same time, Congress began requiring quarterly briefings about the military's cyber operations as well. And now Congress is poised to

extend both models, through pending legislation that likely will became law before 2017 ends. Here is the description of that legislation that I recently posted at Lawfare:

> ***Section 1631: Notification Requirements for Sensitive Military Cyber Operations and Cyber Weapons***
>
> The first major part of this section will add to the growing SASC/HASC oversight legal architecture, adapting the "sensitive military operations" system applicable to kill/capture operations outside areas of active hostilities and applying it to certain cyber operations. As I've noted previously, it helps to think of these SASC/HASC notification systems as analogous to the notification requirements (running to SSCI and HSPCI) relating to covert action.
>
> So, what would section 1631 require? SecDef will have 48 hours to give written notice to SASC and HASC of a qualifying "sensitive military cyber operation." But what counts?
>
> An SMCO is a cyber operation that meets these conditions:
>
> 1. Carried out entirely by the armed forces
>
> 2. With the intent to have a "cyber effect outside a geographic location" where US armed forces are "involved in hostilities" or where "hostilities have been declared by the United States"
>
> 3. Offensive in nature, or else a defensive measure conducted outside DOD networks in order to "defeat an ongoing or imminent threat"
>
> 4. Not a training exercise conducted with consent of impacted nations
>
> 5. Not covert action.
>
> Note that this would pick up some but not all CYBERCOM operations constituting "traditional military activities" (TMA being an important exception to the covert action definition, and thus a category allowing for unacknowledged operations without reporting to SSCI & HPSCI). I say that because you could have a TMA-qualifying computer network operation that does not meet the offense/defense requirement noted above.
>
> Also note that there is a clause at the end of this section confirming that it is not intended to be read as conferring any new authority to act, nor as altering War Powers Resolution obligations (of course, under prevailing executive branch understandings of the WPR's triggers, a computer network operation would not likely set off those triggers anyway!).
>
> And what about the second major part of 1631? It would create an obligation for DOD to give SASC and HASC written notice, quarterly, of DOD reviews of the compatibility of cyber weapons with international law, as well as specific notice of the use of such reviewed cyber weapons within 48 hours of that use. Looks to me like SASC and HASC are concerned about the international law analyses arising during these weapons reviews. Perhaps something to do with third-country effects?
>
> **Section 1632 – Modification to Quarterly Cyber Operations Briefings**

> What about DOD computer network operations that don't qualify as SMCOs? Well, there is still the quarterly briefing process under 10 USC 484, which under this new section 1632 would become more granular in terms of describing (on a command-by-command basis) cyberspace operational activity that the commands conducted and that were directed at the command, along with an "overview of authorities and legal issues" associated with those operations. Seems an excellent idea for smoking out legal obstacles (including the possibility of confusion over the applicable law, which I suspect is part of what motivated that language).

Consider the following:

> *16. What are the pros and cons of adopting the SMCO reporting system?*
>
> *17. Why do you think Congress is so interested in DOD's legal analyses?*

III. CRISIS SIMULATION

With Units I and II under our belts, the stage will be set to integrate our accumulated knowledge in a practical setting. In the final class meeting we will conduct a crisis simulation exercise—a role-play simulating an unfolding cybersecurity crisis—that will give you a unique opportunity to work in teams to demonstrate, and practice with, what you have learned.

14. December 6 – Crisis Simulation