:The User, the Superuser and the Regulator
The Plurality of the State in Cyber

Eldar Haber[*] and Amnon Reichman[**]

… Modalities of Regulation

Regulation could be understood as situated along several axes. One such axes is the measures the state deploys in order to implement the policies adopted. These measures entail the enforcement regime that the state decides to put in place, and the rationale and "legal complex" that follows. We call this a modality of regulation, and there are six of them…

But before we turn to the six modalities, an important distinction between the state as a regulator and a state as actor should be drawn. The state may act directly, not in the capacity of the regulator, but in its direct executive capacity. When the state builds a road, or combats a disaster, or purchases a certain good, it does not draw upon a legal source that empowers it to regulate; it does not issue a legal norm, nor an accompanying implementation and enforcement regime. In the context of cyber, the state may act as a user, namely as just any other entity conducting its business online, by posting something on Facebook, using Twitter or searching on Google. Or it can act as a superuser, relying upon its vast resources, and thus directly influencing the activities on many. For example, it can deploy far-reaching systems of surveillance… or it can decide that any contract with the state should include certain terms that directly affect standards of cybersecurity.

…

Another cautionary comment is that the notion of "leaving matters to the market" is itself a regulatory decision (and therefore it is NOT deregulation). As will be explained further, the market relies on forms of civil liability (contract, property and torts), which, from the perspective of the regulation, is a modality.

….

We now turn to the six modalities of regulation: Regulation through information, licensing, civil liability, criminal liability, taxation and insurance. These modalities can be used in regulation of any field. The state can deploy them separately or combined. As an example, consider regulation of driving. In such form of regulation, the state could, and often does, deploy a combination of all six modalities. It deploys regulation through information when it places duties on the car industry to discourse certain information, and it places certain information-related duties on itself, usually (but not exclusively) via Freedom of Information acts; It requires drivers to obtain licenses and permits to drive vehicles; it imposes civil and criminal liability to various forms of driving and causing accidents; it uses taxes to control the prices of cars, car parts, and certain roads and highways; and it forces drivers to obtain various types of insurances. These six – and only six – modalities are the regimes available to the state in Cyber, and in any other field, as well. The only other modalities that interests with these six addresses the availability of alternative dispute resolutions (ADRs)….

Each of these regulation modalities could potentially regulate cyber activities to some extent. But beyond hypothetical scenarios, each of these types is actively used in today's cyber regulation. This is where the plurality of the state comes to play. The state as a regulator regulates itself as a user, a superuser and a regulator. Furthermore, as we further show, the plurality of the state creates tensions between regulators (different state agencies) and between other superusers. Mainly, it creates nonlinearity and inconsistency in regulation that could lead to suboptimal regulation.

1. *Regulation through Information*

Regulation through information is a broad type of regulatory mechanisms that relies mostly on the notion that individuals can make more educated choices when provided more information.[1] Under such regulatory modality, the "discloser" is provides the "disclosee" information (as stipulated by the regulation), and the later can then make better decisions for herself. In that respect, this modality relies on the Market, in assuming that people will pursue and optimal course if provided adequate information. Regulation through reduces the asymmetry of power of the held by the "discoler" to control the "disclose".[2]

Regulation through information could assist in solving one of the biggest challenges in cyber-regulation: Information gaps. If individuals, for example, will be able to know which cybersecurity measures companies are using, they can choose whether to become their costumers or not (in non-monopolistic markets). Similarly, if consumers will know what exactly is done with the data the corporation harvests from their interactions, or what the value of this data to the corporation is, they may be better situated to make an informed decision regarding the authorization of such uses. But at the same time, consumers might not be well equipped to make educated decisions in such a complex environment. Information could either be too "technical" or there could be too much of it.[3]

There are various forms of data regulation which could take place in cyber. The state can oblige users to disclose whether they encountered a cyber-attack, when such attack occurred, and, to the best of their knowledge, through which means. This type of data regulation is commonly known as *data breach notifications*.[4] Moreover, the State could oblige companies, or even individuals to disclose information about their usage of technology, e.g., if they are using security measure and which measures they are using.

Another aspect, which applies to both users and superusers is data retention. The regulator could oblige companies to ensure the accuracy of the personal information they retain; limit their ability to use the stored information for specific purposes; limit the duration of data retention; require prior consent to collection and retention; etc. By such type of regulation, the regulator can control the information market to some extent. It could protect individuals from the possibility of cyber-attacks that could lead to data theft.

---

[1] For examples of disclosure requirements set by legislation, see Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA L. REV. 647, 649-50 (2011).

[2] *See generally*, Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA L. REV. 647 (2011); OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2013).

[3] *See* Cass R. Sunstein, *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349, 1369 (2011) (noting that "even accurate disclosure of information may be ineffective if the information is too . . . overwhelming to be useful"); Karen Bradshaw Schulz, *Information Flooding*, 48 IND. L. REV. 755 (2015) (arguing that "information overload" could be harmful).

[4] For a full list of state-by-state statutes of data breach notifications, see *State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated June 11, 2015).

A third aspect could be in the form of reports. The regulator could oblige both the executive, Congress and companies to issue reports on cybersecurity and the usage of surveillance methods. Such obligations would not necessarily be equal to all parties. For example, the legislature could oblige a particular agency within the executive but not others. A similar approach could also apply to companies.

Mandating companies to disclose information on cyber-attacks could improve the nation's cybersecurity.[5] The state, as a regulator, could analyze cyber-attacks, and improve the resilience of both superusers and users, including itself.

But such regulation could also be crucial for consumers, especially in the cyber realm. When consumers possess no knowledge of which companies are "safe", due to asymmetric information, they could not make efficient choices. Disclosure regulation can restore such balance in the market to some extent.[6] Eventually, however, due to the massive amounts of users and potential threats, and the potential complexity of understanding the ramifications of cyber incidents (meaning that many lack the expertise to evaluate cybersecurity), such data disclosure is not free of difficulties. From the user's perspective, such information disclosure will not necessarily decrease their bounded rationality; too much information is not necessarily beneficial either.[7]

Even if information disclosure could aid in consumer protection and thereby increase cybersecurity, it unlikely it could, on its own, fully alleviate the concerns cyber threats generate…

2. *Licensing*

The second regulation modality is that of licenses. The usage of licenses to regulate behavior is common. Many users need licenses to operate: Drivers, doctors, psychologists, brokers, attorneys, manufactures, exporters and importers, and many others.[8] Even marriage requires a license.[9] Some superusers also need licenses to operate. … Communication companies for example might be required to obtain a license to provide services or operate facilities.[10]

---

[5] Data breach notifications statues in the U.S. are state legislated and require private and government entities to notify individuals of security breaches of information involving personally identifiable information, unless such information was encrypted. This form of "encryption safe harbor" could lead companies to better secure their information with encryption (as long as the encryption is optimal), and incentivize encryption industries to work on technological solutions to cyber problems. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 297 (2014) (describing the "encryption safe harbor" in the U.S.).

[6] *See generally*, Michael J. Fishman & Kathleen M. Hagerty, *Mandatory Disclosure, in* 2 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 605 (Peter Newman ed., 1998).

[7] Individuals have limited time and cognitive energy, and thereby will often not look for the entire set of information, but rather information which is "good enough" to make a decision, using thumb rules or "satisficing" behavior. This phenomenon is referred to as “user embeddedness.” *See* David Weil, Archon Fung, Mary Graham & Elena Fagotto, *The Effectiveness of Regulatory Disclosure Policies*, 25 J. POL'Y ANALYSIS & MGMT. 155, 158 (2006). For more on law and market behavior, see, e.g., Avishalom Tor, *Understanding Behavioral Antitrust*, 92 TEX. L. REV. 573 (2014).

[8] *See, e.g.*, 18 U.S.C § 923 (2012) (licensing requirements for bearing and using firearms and ammunition).

[9] For a full list of updated marriage statutes, see Marriage laws, LII https://www.law.cornell.edu/wex/table_marriage (last visited Oct. 15, 2015).

[10] For example, the FCC requires providers of telecommunications services to or from the United States to receive an authorization under Section 214 of the Communications Act of 1934 (Pub. L. No. 73-416). *See*

Licenses may thus be relevant for cyber activities as well. Users may be required to obtain licenses if they wish to engage in form of commerce that could involve cyber-attacks. Import is a good example. The state can oblige importers to obtain a license determined by various factors, e.g., the product, the country that the product is imported from, the end-use and the potential end-user. By such licenses, the state as a regulator can control, at least partially, which components enter its domain, and furthermore, which uses are permitted for such products. Licenses or permits may also be relevant for regulating the labor market surrounding cybersecurity, by issuing licenses for certain professions….

Regulation through licenses could also apply on superusers, beyond import and export requirements. The most common license, or permit, relates to the market share of the superuser, as it seeks to purchase other companies. Other licenses may relate to restrictions of use of technology, data retention, collaboration or sharing of information, surveillance, and cyber-retaliation. In that way, the state can limit a superuser, such as Google or Facebook, by placing certain conditions on their use of their powers (while operating and/or offering services in the U.S.). Licensing could also reduce the possibility of future superusers by creating high barriers for market entry, and "control" the number of superusers (and increase the obligations they face, as superusers).

Nevertheless, while licensing could regulate behavior in the cyber realm for some extent, it also may face some difficulties if taken as the sole solution for cyber threats… To some extent, mainly when we think of cyber-attacks and defense, a user's activity could be hazardous. Carless use of computers and mostly computerized networks could endanger themselves or even other users, and it appears impractical to license all users or all products users may purchase which bear on cyber threats.

3. *Civil Liability*

Another modality of regulation is civil liability. This modality is sometimes takes as a base-line of “the market”, and thus not fully understood as a regulatory modality. When the state regulates the terms of contracts it will enforce, or the tort liability that may be associated with certain actions, it is regulating the field, through private action. In our context, the regulator may impose civil liability on cyber-related activities, and thus regulate conduct. Such form of regulation can be performed by using and/or legislating various forms of torts, or by designing the legality of contractual terms that seeks to mitigate or foreclose liability. Similarly, the state may regulate the transferability of “property” (which is a form of license by state, as viewed from a regulatory perspective). Under tort law, the state can designate the level of liability -- intentional, strict and/or negligence – for cyber-related activities. It may also deploy potential punitive damages. By imposing civil liability, the regulator seeks to ensure that individuals and corporations are incentivized to optimally avoid hazardous behavior. The reach of civil liability could well extend beyond the "direct" injurer. The state can impose civil liability on third-parties, i.e., intermediaries, and thus expend the reach of such modality. Victims could seek relief claiming breach of a duty of care to maintain a secure network and/or a breach of fiduciary duty to keep data secure, and the state itself may be authorized to sue in private law for damages its citizens suffer.[11]

---

47 U.S.C. § 214 (1976).

… [I]n some instances, civil liability could be efficient … but there are also many drawbacks of solely using such modality. Civil liability applies *ex post facto*,[12] and it relies on private enforcement (by users, companies or the state). If breaches occur but lawsuits are not filed, enforcement will be suboptimal at best, and thereby the state will not achieve the desired goals. This element is crucial in cyber-related activities. In many instances, the victims will be either unaware of the cyber activity which injured them; unable to detect and/or attribute the attack to an attacker and locate him;[13] unequipped to assess the damages; fear lengthy and contentious litigation with potential high legal costs; face jurisdictionally limitations; and the insolvency of judgment-proof attackers.[14] In addition, when the time between exposure to risk and the appearance of symptoms is very long, potential deterrence could be weakened. The damage in many forms of cyber-activities can occur much after the activity has ended. Therefore, causation would be difficult to assess, and could also be problematic in some countries due to a limitation period set by the law. … Additionally, holding intermediaries liable for cyber-attacks could be prove problematic and may have negative effect on the market and on innovation.[15] Finally, civil damages could be problematic for many other reasons. Even high fines may not necessarily affect big companies which are considering such potential fine as a "cost of doing business" (which may later find its way to the customer). High fines could nevertheless drive small companies out of the market. If fines are set too low, then they will not likely achieve their goal…

4. *Criminal Liability*

Perhaps the most aggressive modality to regulate behavior is that of criminal law, considered by many as a last resort.[16] The usage of criminal law could have many purposes,[17] but in sense of regulating behavior, it relies on the notion of deterrence.[18]

---

[11] *See* Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 208 (2006).

[12] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 460 (2012).

[13] *See supra* note 20.

[14] When the regulated entity is judgment-proof, lacking sufficient assets to pay fully for the damages he causes, civil liability will not likely fulfill its purpose.

[15] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 456-57 (2012) (arguing that "[e]ncouraging injured parties to sue the intermediaries who are arguably negligent in some manner also raises a slew of problems.").

[16] Nils Jareborg, *Criminalization as Last Resort (Ultima Ratio)*, 2 OHIO ST. J. CRIM. L. 521, 525 (2005) (quoting GONTHER STRATENWERTHM STRAFRECHT: ALLGEMEINER TEIL 1: DIE STRAFRAT 40 (4th ed. 2000), who argues that "Punishment" [in the sense of criminal law – E.H & A.R.], should be used only where other measures, in particular private law and administrative law measures, fail); *Cf.* Malcolm Thorburn, *Constitutionalism and the Limits of the Criminal Law*, *in* THE STRUCTURES OF THE CRIMINAL LAW 101 (Antony Duff et al. eds., 2011) (arguing that criminal law is not *ultima ratio* in the sense that we ought to use regulatory instruments other than the criminal law to control behavior if we can. Rather, "it is ultima ratio in the deeper sense that it is a necessary last resort (or backstop) to the whole project of living together with others under law.").

[17] Criminal punishment is usually justified on grounds of incapacitation, desert/retribution, deterrence, rehabilitation, and/or restorative justice. *See* ANDREW ASHWORTH, SENTENCING AND CRIMINAL JUSTICE 77-91 (2010); GEORGE P. FLETCHER, RETHINKING CRIMINAL LAW 409 (2010).

[18] *See* ANDREW ASHWORTH, SENTENCING AND CRIMINAL JUSTICE 77-91 (2010); GEORGE P. FLETCHER, RETHINKING CRIMINAL LAW 409 (2010); Paul H. Robinson, *Criminalization Tensions: Empirical Desert*,

Beyond deterrence, some individuals and companies could comply with the law due to criminal law's expressive value. Under this approach, sanctions can regulate the behavior of individuals which view any criminal prohibition as a wrong, simply because it is criminal, even without clear justifications for the criminalization.[19]

Generally, the state can impose criminal liability on both users and superusers.[20] Individuals are probably the more natural candidates for criminal liability, but in the US corporations are also subject to criminal sanctions.[21] The latter occurs when their employees and/or agents commit a crime on their behalf.[22] While corporations cannot be imprisoned, they can pay fines and/or victim restitution, which may expose the corporations the loss of all their net assets.[23] They man be placed on probation;[24] face forfeiture;[25] as odd as it sounds, do community service;[26] and endure other penalties.[27] In addition, the criminal sanction could carry stigma and/or loss of reputation.[28]

Depending on the nature of the cyber activity in question, the State can impose criminal sanctions on various players…. The most likely candidates for criminal liability are those who unlawfully and knowingly access a computer without authorization, i.e., hack.[29] Under the presumption of deterrence, imposing high sanctions could deter some individuals from hacking.[30] Superusers can also be liable. The state, for example, can use its capacity to attack other superusers, whether states or companies. By using criminal

Changing Norms, and Rape Reform, in THE STRUCTURES OF THE CRIMINAL LAW 186, 187 (Antony Duff et al. eds., 2010).

[19] For the positivistic approach to criminal law, see Henry M. Hart, *The Aims of the Criminal Law*, 23 LAW & CONTEMP. PROBS. 401, 404 (1958); DENNIS J. BAKER, THE RIGHT NO TO BE CRIMINALIZED 2 (2011).

[20] Congress regulated cyber-related activities (though not necessarily intentionally) by criminal sanctions through many acts of legislation. Few examples are: The Electronic Communications Privacy Act (codified as amended at 18 U.S.C. §§ 2510–2711 (2012)) (providing criminal sanctions [and civil damages] for unauthorized interception or disclosure of electronic communications); The Computer Fraud and Abuse Act (18 U.S.C. § 1030 (2012)) (punishes "computer crime"); The Economic Espionage Act (18 U.S.C. § 1831 (2012) (provides criminal sanctions [and civil damages] for "economic espionage."). *See* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 87-92 (2001); David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907 (2013).

[21] For more on corporate criminal liability, see, e.g., Harvey L. Pitt & Karl A. Groskaufmanis, *Minimizing Corporate Civil and Criminal Liability: A Second Look at Corporate Codes of Conduct*, 78 GEO. L.J. 1559 (1990); V.S. Khanna, *Corporate Criminal Liability: What Purpose Does It Serve?*, 109 HARV. L. REV. 1477 (1996); Frederic P. Lee, *Corporate Criminal Liability,*
28 COLUM. L. REV. 1 (1928).

[22] Consequently, the employees and/or agents that are liable could also face prosecution and punishment. See, e.g., in the U.S., United States v. Agosto-Vega, 617 F.3d 541, 552-53 (1st Cir. 2010); United States v. Philip Morris USA, Inc., 566 F.3d 1095, 1118-119 (D.C.Cir. 2009); United States v. Singh, 518 F.3d 236, 249 (4th Cir. 2008).

[23] *See, e.g.*, in the U.S., U.S.S.G. §8C1.1.

[24] *See, e.g.*, in the U.S., U.S.S.G. §8D1.1(a)(7); 18 U.S.C. 3551(c).

[25] *See, e.g.*, in the U.S., U.S.S.G. §§8E1.2, 5E1.4.

[26] *See, e.g.*, in the U.S., U.S.S.G. §8D1.3.

[27] *See* V.S. Khanna, *Corporate Criminal Liability: What Purpose Does It Serve?*, 109 HARV. L. REV. 1477, 1497-99 (1996).

[28] *See* V.S. Khanna, *Corporate Criminal Liability: What Purpose Does It Serve?*, 109 HARV. L. REV. 1477, 1499-512 (1996).

[29] *See, e.g.*, in the U.S., 18 U.S.C § 1030 (2012).

[30] There are various deterrence models, but the "classic" model would also require the presence of effective enforcement and the perceived benefits from hacking. *See generally*, Becker, *supra* note 153.

sanctions, state officials or company's employees could be criminally liable for cyber-attacks, and therefore could be deterred from hacking.

Regulators can also use criminal sanctions to regulate cyber defense. .... Such regulation could affect companies which import or export cyber-related technologies. It could also apply on owners of critical infrastructures,[31] and anyone who provides services that could be compromised. ….

Lastly, the regulator could impose criminal sanctions for anyone who takes part in the surveillance process. From manufactures and importers of equipment and software designed to enable unlawful surveillance to companies and individuals who engage in surveillance. On the practical side, such modality in this sense would mostly apply on superusers, capable of conducting surveillance. But the State can use it in an attempt to deter other superusers from conducting surveillance.

Whether criminalization of cyber-related activities is justified is a complex question,[32] which is beyond the scope of this article. Our intention here is not to assess whether the theoretical frameworks of criminal law justifies criminalization, but rather to

---

[31] Implementing security measures could be most crucial when protecting critical infrastructure. The state can impose criminal sanctions on operators of CI which do not comply with governmental instructions of protecting their assets, and thereby, risking the state and civilians. This could include, inter alia, mandating the usage of state-verified equipment, implementing security measures, hiring security personal, sharing information in real-time or other measures.

[32] Reviewing academic literature reveals that criminalization theories are diverse and inconsistent. Theories have either focused on the notion of potential or actual *harm* to individuals and to society, and/or whether the conduct is inherently immoral and should be criminalized due to its *wrongful nature* (see JOHN STUART MILL, ON LIBERTY 8-9 (New York: Penguin 1982) (1859) (arguing that the only purpose for which power can be rightfully exercised over any member of a civilize community, against his will, is to prevent harm to others). The harm principle appeared in a more moderate liberal position after being developed further by *Joel Feinberg* which argued "[i]t is always a good reason in support of penal legislation that it would be effective in preventing (eliminating, reducing) harm to persons other than the actor (the one prohibited from acting) and there is no other means that is equally effective at no greater cost to other values." *See* JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW: HARMLESS WRONGDOING xix (1988)). Legal moralism advocates for the criminalization of a morally wrongful conduct, perpetrated with a culpable state of mind due to its wrongfulness. *See* ANTONY DUFF, LINDSAY FARMER, SANDRA E. MARSHALL & VICTOR TADROS, THE TRIAL ON TRIAL, TOWARDS A NORMATIVE THEORY OF THE CRIMINAL TRIAL 17 (2007) (explaining the legal moralism approach to criminalization). Another approach, advocated by a few legal systems which primarily emphasizes the protection of social values, suggests that criminalizing behavior should mostly rely on identifying an important *protected social interest*, which could justify the reason why a particular conduct should be prohibited by criminal law; *See, e.g.*, Mordechai Kremnitzer & Khalid Ghanayim, *Proportionality and the Aggressor's Culpability in Self-Defense*, 39 TULSA L. REV. 875, 879 (2003) (identifying social interests as interests that serve a function and not merely as abstract values). In recent years, have we witnessed the emergence of a more substantive academic discussion on criminalization, and few structured principled approaches to criminalization were suggested by scholars. The *principled* approach strives to ensure that certain standards are met before criminalizing a conduct and sets limits on the state's power to enact criminal legislation. Jonathan Schonsheck suggested three elements: *Principle filter*, *presumptions filter*, and *pragmatics filter*. Douglas Husak argues that criminal laws must satisfy seven different internal and external constraints (to criminal law). Asaf Harduf offers an analytical examination of criminalization through a *ladder of criminalization*. *See* JONATHAN SCHONSHECK, ON CRIMINALIZATION (1994); DOUGLAS HUSAK, OVERCRIMINALIZATION: THE LIMITS OF THE CRIMINAL LAW (2008); Asaf Harduf, *How Crimes Should Be Created: A Practical Theory of Criminalization*, 49 CRIM. L. BULL. 31 (2013). For more on criminalization theories, see, e.g., NINA PERŠAK, CRIMINALISING HARMFUL CONDUCT: THE HARM PRINCIPLE, ITS LIMITS AND CONTINENTAL COUNTERPARTS (2007); Paul H. Robinson & John M. Darley, *The Utility of Desert*, 91 NW. U. L. REV. 453 (1997); Andreas von Hirsch, *Harm and Wrongdoing in Criminalisation Theory*, 12 CRIM. L. & PHIL. 1 (2012).

examine whether criminal law is an optimal legal tool to regulate cyber activities. Hence, the more fundamental question here is whether criminal sanctions could affect individual's behavior, and what is the trade-off of such regulation.[33]

…

The support for deterrence as a form of behavior regulation had been widely criticized in academic literature. [34]Economic analysis of crime relies, inter alia, on human *rationality*. Under common deterrence theory, assuming that people are rational utility maximizers and risk neutral, a decision to commit a crime is much like any other decision people make.[35] Decisions are largely based on the net-benefit, which is comprised of a cost-benefit analysis: Individuals weigh the benefits of an act against the probability and magnitude of punishment,[36] and only comply with the law when the benefits of compliance outweigh their costs. Specifically, an act will be deterred when expected costs are higher than expected benefits.

The main problem of the deterrence theory is that it does not take into account non-rational actors, and thus does not apply to all viable players in the field. Hence, if individuals are not risk-neutral, i.e., they are either risk-preferring (with the same expected value, always prefer the maximum potential return of their choice) or risk-averse (with the same expected value, always prefer the choice with the least risk), deterrence will not likely alter their behavior. In the cyber-realm, it seems highly crucial to make this distinction. Some users and superusers will probably act as rational actors, and deterrence could be achieved to some extent. But the cyber realm also includes non-rational actors. It is part of the nature of hacking, isn't it? Nonconformity of some sort.

Second, *information and knowledge gaps* of many users and companies regarding the scope and possible ramifications of their actions and the possible sanctions they might face if caught may hinder optimal implementation of this regime. …

Third, *enforceability*. The difficulties of attribution, detection and jurisdiction widely apply to both private and public enforcement. The bottom line is that as long as enforcement rates are low, it would be highly difficult to achieve deterrence.

At the end of the day, whether to impose criminal sanctions on companies relies on the extent to which public enforcement is conducive to ensure the internalization of cyber-security costs.[37] As a general argument, criminal law is preferable in those

---

[33] Paul Robinson & John Darley argue that a particular rule can be expected to change behavior only when three assumptions are satisfied: awareness of the rule; the knowledge must be able to influence the behavior at the moment decisions are made; and that the individual must believe that the perceived costs outweigh the perceived benefits of offending. *See* Paul H. Robinson & John M. Darley, *Does Criminal Law Deter? A Behavioral Science Investigation*, 24 OXFORD J. LEGAL STUD. 173 (2004).

[34] Deterrence theory and economic analysis of crime had been widely criticized over the year. *See, e.g.*, Dan M. Kahan, *The Theory of Value Dilemma: A Critique of the Economic Analysis of Criminal Law*, 1 OHIO STATE J. CRIM. L. 643 (2004; GEORGE P. FLETCHER, THE GRAMMAR OF CRIMINAL LAW: AMERICAN, EUROPEAN, INTERNATIONAL 59 (2007) (arguing that law and economics "have nothing to say about substantive criminal law.").

[35] Becker, *supra* note 153, at 83-85.

[36] JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION 178-88 (Oxford: Clarendon Press, 1996) (1789).

[37] *See, e.g.*, William M. Landes & Richard A. Posner, *The Private Enforcement of Law*, 4 J. LEGAL STUD 1 (1975); A. Mitchell Polinsky, *Private Versus Public Enforcement of Fines*, 9 J. LEGAL STUD. 105 (1980).

instances civil or administrative laws fall short from achieving the internalization of the costs of an unlawful act,[38] and criminal law achieves optimal enforcement.[39]

Lastly, the *ex post factor* nature of the modality should be recognized.[40] Even if enforcement is optimal, the fact that someone will be punished after a successful attack on critical infrastructure will not necessarily reduce the potential damage, as not all attacks will be prevented…

5. *Taxation & Subsidy*

Taxation is another modality of regulation. It is a form of distributive economic incentive, which could be deployed to subtract or add value pursuant to certain non-libelous conduct or outcome. By setting taxes and subsidies, the state can regulate markets and behavior of consumers and industry without setting direct civil or criminal liability (although usually, but not always, non-compliance will trigger such liability). The State could provide tax credits and/or deductions for companies that comply with regulation, or for individuals (users) that that perform certain tasks or reach certain standards. For example, positive or negative taxes may be attached to the implementation of approved cybersecurity measures.

Taxation could also serve as a more "direct" form of incentive. The regulator can offer grants to companies and provide direct federal funding for investment in cybersecurity products and services. It could offer tax benefits for employers in the cyber industry depending on various factors set by the state.[41] Beyond direct funds, the State can grant companies and individuals cyber-related services in exchange to compliance with cybersecurity measures.[42] Also, they can offer subsidies, and directly purchase cybersecurity products and services for framework owners and operators. This could be done in its role as a superuser, but could also be set by legislation, and hence, in its role as a regulator.

Due to the usage of the user/superuser cyber taxonomy, taxation represents an interesting example in the cyber sense. The state, as a regulator, sets taxes that apply to

---

[38] ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 452 (4th ed. 2004); If one person's actions impinge negatively on one or more third parties, it results in negative externalities. For example, a polluting factory could potentially cause a negative externality if it adversely affects neighbors. If the state imposes liability on the factory owner, the consequences become internalized on whether to build the factory or how to handle possible pollution. For a similar argument, see Roger Bowles, Michael Faure & Nuno Garoupa, *The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications*, 35 J.L. & SOC. 389, 396-97 (2008). In addition, the Coasean approach to externalities will justify public enforcement when high transaction costs between parties are likely to fail. *See* Ronald Coase, *The Problem of Social Cost*, 3 J. LAW & ECON. 1 (1960); Guido Calabresi & Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

[39] Robin Andrews, *Copyright Infringement and the Internet: An Economic Analysis of Crime*, 11 B.U. J. SCI. & TECH. L. 256, 262 (2005).

[40] *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 460 (2012).

[41] See, e.g., in Israel, where the government approved a significant tax break for cyber companies that move to the newly formed "national cyber park" in the city of Be'er Sheva. *See Cabinet approves tax break for National Cyber Park*, MFA (July 6, 2014), http://mfa.gov.il/MFA/PressRoom/2014/Pages/Cabinet-approves-tax-break-for-National-Cyber-Park-6-Jul-2014.aspx.

[42] For example, the state could offer prioritized cybersecurity technical assistance from the federal government for companies and individuals that implemented cybersecurity standards.

both users and superusers. It is a modality in which both users and other superusers directly fund the state's activities as both a regulator and a superuser. These taxes could aid the state as a superuser to increase resources, while potentially weakening other superusers.

But taxation raises many similar difficulties ....

6. *Insurance*

Insurance is a risk-sharing mechanism that compensates for loss from funds collected in relation to risk. The State regulates many fields through insurance. In the cyber realm, the state could oblige purchasing liability insurance.[43] Service providers and operators of critical infrastructure might be required to purchase liability insurance as well. Such insurance will protect these companies and CI operators from bearing full costs arising from negligence claims made by a client, and damages awarded in such a civil lawsuit. In other words, the losses associated with computer intrusions could shift from individuals and companies to the insurance companies.[44] ... For insurance to work, it must rely on relatively accurate tables of risks associated with certain states or activities, as well as on tables the values expected to be lost (and the ability of the market to support a premium that will offset these losses, or segments thereof).

Insurance markets generally address cyber regulation in a familiar manner. ….Insurance is probably a good solution to some extent,[45] but informational deficiencies may hinder its efficiency. Moreovoer, it is not clear it is suitable to address harm to critical infrastructure. Suppose that the owner of a large power utility decides not to invest in cybersecurity, but rather purchase insurance. After a successful attack on the utility, casting large amount of individuals into darkness for a month, the owner seeks to recover his losses.[46] But what about the harm to costumers and the potential risks for national security due to the lack of electricity? For the model to work, customers may have to have insurance as well, although some risks may be too high or too unpredictable to be insured. Conversely, some risks may be too rare (but devastating when they occur), resulting in customers seeking to avoid insurance if they think the risk will not materialize in their lifetime.

---

[43] Example of such "hacker insurance" exists. *See, e.g.*, Karen E. Klein, *Insurance for When You Get Hacked*, BLOOMBERG (Aug. 28, 2014), http://www.bloomberg.com/bw/articles/2014-08-28/cyberliability-insurance-for-when-your-business-gets-hacked; Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L. J. 2261, 2287-88 (2003); Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 208-09 (2006).

[44] In the cyber-realm, these damages could incur from, inter alia, data beaches, network and equipment damages, etc.

[45] Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 351 (2006) (arguing that "cyber insurance [is] an extremely promising route to solving the identified market failures in software system security."); *Cf.* Nikhil Shetty, Galina Schwartz, Mark Felegyhazi & Jean Walrand, *Competitive Cyber-Insurance and Internet Security, in* ECONOMICS OF INFORMATION SECURITY AND PRIVACY 229 (2010) (finding that in the presence of competitive cyber-insurers, incentives for good security practices only deteriorate).

[46] For a similar example of how insurance fails to properly regulate critical infrastructures from cyber-attacks, see Lior Frenkel, *NIST Framework Misses the Mark on Risk Assessment*, WATERFALL (Dec. 26, 2013, 10:09 AM), http://waterfall-security.blogspot.co.il/2013/12/nist-framework-misses-mark-on-risk.html.