

Dear Information Society Seminar participants,

I am honored to be given the opportunity to discuss with you parts of my dissertation entitled, “A Paradigm Shift in Online Policing - Designing an Accountable Policing”. This project includes four chapters: First, “Digital Crime Scene” offers an analysis of the unique attributes of cybercrime; second, “Paradigm Shift in Policing” discusses the emergence of a new CyberPolicing model as a response to Cybercrime. This new model is proactive and operates by a complex institutional structure, and is gradually replacing the traditional Law Enforcement model of policing; third, “Accountability in the New Policing Model” analyses the failure of current legal, technological and institutional structures to control the emerging model of online policing. It questions whether Pre-Authorization rules, that are predominant in criminal procedures, are adequate in controlling the new policing operations. Therefore, it encourage the adoption of Privacy Enhancing Technologies and A System of Continuous Accountability to control policing; and, Fourth, “Rethinking Policing Accountability – Watch the Watchers” prescribes guidelines for “Accountability Mechanisms” (legal, technological and institutional) for the new policing environment. It portrays the design of these mechanisms which can facilitate a culture of policing accountability.

Given the broad coverage of this project, I have decided to focus the seminar’s discussion on the “Paradigm Shift in Policing”. The suggested reading includes a few short excerpts from Chapter 2 which were combined together. I also assigned a short introduction from Chapter One to provide some background about the Digital Crime Scene. In the seminar, I will further address the findings of Chapter One before starting the discussion on the Paradigm Shift. It is still work-in-progress and I would very much appreciate your comments. If you happen to find interest in other chapters of the projects, and mainly the Accountability System, please contact me or download the papers from the Information Society Project’s website, Yale Law School.

I am looking forward to the discussion,

Nimrod Kozlovski

## **A Paradigm Shift in Online Policing - Designing an Accountable Policing**

*[Excerpt from chapter one – introduction- p. 1-5]*

### ***Chapter One - Digital Crime scene – Rethinking Crime***

#### **I. Introduction**

This chapter introduces the digital crime scene. It encourages us to analyze the connection between the design of the crime scene, common criminal behaviors and the attributes of the committed crimes. It posits the argument that there is a close nexus between the design of the environment and the patterns of criminal behavior. In the online environment, crime possesses unique attributes. We need to examine these attributes to properly analyze their effect. The policing model, of public reactive law enforcement, which society has chosen, is based upon certain assumptions on how crime is committed. We need to find whether these assumptions are still valid with the new attributes of crime. If they are not valid anymore, we will have to question whether we need a different policing model that fits the new attributes of crime.<sup>1</sup>

---

<sup>1</sup> This chapter takes somewhat different method than the common method of examining cybercrime. Researchers commonly compare cybercrime to offline crime and examine whether cybercrime presents a unique attribute which does not exist offline. I prefer to examine first hand cybecrime to analyze its attributes. When offline crime can serve as a good analogy to understand it I may use this analogy. However, I do not find an inherent importance in the comparison to offline crime. Even if an attribute of online crime can be found somehow in offline crime, it is no indication that the offline and online crime are similar. It is not the novelty of attributes which sometimes makes a difference but the salience of certain attributes which makes it qualitatively different. Anonymity, for example, could be partly achieved offline by wearing a mask, but does it mean that offline anonymity and online anonymity are similar? Certainly not. Anonymous crime is a rare and practically negligible incident in the “real world”. To the contrary, online crimes are mostly anonymous. It is the salience of anonymity online which makes all the difference. This carries significant importance for the policing response to crime. If anonymity is negligible offline, the policing model can be structured around this assumption. If in contrast, anonymity is the normal condition of online crime, the policing assumption is no longer valid and we may need to search for a different policing model. In other words: research method which focuses on comparing offline to online crime is likely to make a logical flow. It is likely to subscribe to the following logic: if we find the same attribute in online and offline crime, we can assume that the policing assumption is still valid. It makes two mistakes: first, as explained, it ignores the importance of saliency; second, it suggests that each attribute can be examined separately. This is wrong. Crime is a complex social phenomenon which can only be understood by complete analysis of all factors combined. Only the interaction between the different attributes can teach us what crime is probable, how it likely to be committed and what will be the possible defense against it. Certain attributes can be combined online, but may be mutually exclusive offline. I prefer, therefore, to examine cybercrime directly and to study the dynamic interaction between its different attributes.

Several scholars have argued that cybercrime is a totally new phenomenon. Cybercrimes are committed by different types of people, require different skills, and often lack traditional motives. Online, people often commit crime for fun or solely for the sake of disruption (e.g. virus spreading or denial of service attack). Crime is committed in a different magnitude and presents existential threats to contemporary society. It renders societal assumptions about crime invalid and requires a separate body of law to handle it.

Yet, other scholars have argued that there is nothing new under the sun. They have challenged the “cyberspace separatism” notion.<sup>2</sup> Crime has always been part of the social experience and will always be part of the social experience. Degrees of social deviance are exercised online just as they are exercised offline. The menu of crimes has not changed dramatically and continues to reflect the same types of socially undesirable behaviors. As the claim proceeds, criminal law has served us in regulating such undesirable behavior offline and will continue to serve us online. Those who subscribe to this notion claim that we just need to amend the law when necessary to capture the deviant behavior when it transforms online. They claim we need only to alter some definitions to adjust to online crime, but there is no need for substantive change.

This chapter contests all of the abovementioned notions. I do not agree with the assumption that cybercrime is totally different or committed largely by new types of criminals, or for a completely different set of motives. Most cybrcrimes are analogous to offline crime and are conducted for the same motives of offline crime.<sup>3</sup> Therefore, we need very little substantive amendments to our definitions of crime to adjust to the new environment. They are required mainly when the targets of the crime are the computer itself or the network. The contemporary trend of criminalizing more online activities has

---

<sup>2</sup> See for example: Christopher M. Kelly, *The Cyberspace Separatism Fallacy*, 34 *Texas International Law Journal* 413 (1999).

<sup>3</sup> There may be some limited new forms of criminal behaviors or crimes which are committed for motives which are uncommon offline. However, even if this is true, these criminal behaviors are peripheral in the overall cybercrime phenomenon. Most of the cybercrime phenomenon is composed of traditional crimes which migrate online or attacks against computer systems for the same motives which are common offline. For a potentially different view, see: Susan W. Brenner, *Toward A Criminal Law for CyberSpace: Distributed Security*, 10 *Boston University Journal of Science and Technology Law* 1, 50 (Winter 2004).

little to do with the unique criminal risks of the new environment. It is more linked to economic interests and attempts to protect winners of the old economy with the shift to the information economy.<sup>4</sup>

So is there really nothing new about cybercrime? I don't think so! I think that cybercrime can be perpetrated in a manner that is very unique requiring special and separate attention. Even if perpetrators of online crime aim to accomplish the same malevolent goals they did offline, they commit crime in a very different manner. The online environment enables people to commit crimes on a different scale and different damage potential with minimal skills, by taking advantage of digitization, automation and distributed design. Online criminals can easily hide their identity, "Digital Traces", and incriminating evidence to escape accountability. Furthermore, cybercrimes are not bound by physical territories and jurisdictions and can inflict severe transnational harm. All these factors change the potential magnitude of crime, the social organization of criminal activity, and the cost-benefit considerations in committing a criminal activity.

As we will see later, the new characteristics of crime should affect the societal response to it. The new crimes no longer fit the operational assumptions of the common model of policing, the reactive public law enforcement. The law enforcement response to crime is structured around certain assumptions about how crime is committed in society. When the patterns of crime change, society needs to reexamine whether the underlying assumptions of policing are still valid. If the assumptions prove to not be valid anymore, society must question whether to change the policing model so as to be efficient in responding to crime.

This chapter aims to present the unique attributes of online criminal behavior. It will enable us in the second chapter to question the validity of the common policing model, the reactive public law enforcement. The focus of the current chapter is a discussion about what cybercrime is and how such crimes are committed. It starts from the basics

---

<sup>4</sup> As we will discuss later, these crimes – such as criminal piracy or attention crimes - are not required by the new environment but are a matter of political choice.

and gradually builds the required body of knowledge that is a prerequisite for a policy discussion. Unfortunately, much of contemporary policy discussion in the field lacks such foundations. The discussion about cybercrime is too often led by myths, unclear definitions, and misconceptions about the technological environment. It is probably because we have not yet adopted our legal and social perceptions to the new conditions of crime.

In an evolutionary process, people have developed the proper intuitions and instincts for crime in their physical environment. The sense of risk, the ability to assess risk and the perception of the potential criminal – all were shaped progressively through time. They are embedded in our behavior, carried through our “social software” and affect the way we design our institutions. At a time of major changes in our living conditions, people have to adopt their sense of crime to the changing profile of risk and its new patterns. With the change from an agrarian society to an urban society, crime patterns changed and so changed the profile of risk. People did not adapt instantly to this change. It took time for the individual and for society to assess the new risks, to acknowledge their new vulnerabilities, and to educate themselves about the new patterns of crime. It took time to acquire the appropriate intuitions and instincts for the new urban crime environment. It also took time to develop the proper individual and collective defense mechanisms against these risks.

With the shift from the urban physical environment to the information environment, we need to go through such a process again; adapt to the new risk profiles and new crime patterns. It is a frightening process. People feel vulnerable and stripped of their natural and social defense mechanisms which enabled them to cope with external risks. How can someone steal my identity? How can I protect my identity? Who is a hacker? Can he read and see everything I do online? How can I differentiate between a legitimate site and a scam? How do I identify a malicious code? Can someone with a click of mouse really flood my city with water or blow up the airplane I am riding? Most of us have no clear idea what the answers might be, but we feel vulnerable. We don't know what the risks are, how to assess them and how to defend ourselves.

Moreover, in the new environment, we lack many of the social signals which traditionally helped us to cope with these unfamiliar risks. We feel alone in an unknown terrain. We seek guidance, but we often receive mistaken or distorted signals about risk which are then amplified by the media, popular culture or self-interested security firms.<sup>5</sup> This is a time when myths arise and misconceptions develop. Policy making at such time is often led by myths and misconceptions more than it is led by facts and a logical analysis of reality. At such time there is a political tendency to act swiftly and to take harsh measures to defend ourselves against these new risks (even if we can not clearly identify them yet). We tend to further criminalize activities, to enact more severe sanctions, to arm the police with new powers, and to trade civil liberties for promises of better security. We may need to take some of these measures, but they must be pursued only after we understand the new crime scene and properly identify our vulnerabilities and our risks. Before we defend ourselves, we are advised to learn what we are defending ourselves from. It would help us to properly assess what defense strategy is likely to solve the problem. Shooting in all directions is normally a bad recipe for fighting an enemy. You first need to know the enemy, its location, patterns of behavior and its weaknesses, to be able to tackle him efficiently. It is time to know the enemy.

---

---

<sup>5</sup> The media has a role in creating “moral panics”. The media is exaggerating the threats of crime by highlighting the most sensational crimes. See more: Steven M. Chermak, *Victims and the News: Crime and the American New Media* (1995); Aric Press & Andrew Benson, *The Police, The Media and Public Attitudes*, in *Measuring What Matters: Proceedings from the Policing Research Institute Meeting*, National Institute of Justice (July 1999).

*[Excerpt from chapter two – introduction- p.75-84]*

## **Chapter 2 – A Paradigm Shift in Policing**

### **1. Introduction**

We are in the midst of a paradigm shift in how we police society. The old paradigm of policing which has dominated modern societies is being replaced online by a new paradigm that carries a distinctively different form. This new model of policing is unlikely to restrict itself to the boundaries of the online world and will gradually become the primary policing model in society. In the last century, most western countries have been accustomed to the “*professional law enforcement model*”. This model is a reactive way of responding to a committed crime with professional public officers. However, a new model is emerging in the online environment, a *cyber-policing model*. It is proactive and operates with a complex hybrid of public and private organizational structure. It changes the paradigm from one of criminal justice to one of security. It favors prevention over detection and punishment.

The process of restructuring policing started to develop off-line almost three decades ago; it has begun to favor new preventive strategies and private security forces. However, the old law enforcement model has fairly strong roots offline. Yet, with the shift to a digital crime scene the old law enforcement model for many crimes is no longer a valid option.

The old model rests on certain assumptions: criminals are deterred by the probability of sanction; investigation is likely to trace back to the criminals and provide evidence for prosecution, and the damages of crimes are of a manageable scale. All these assumptions – which may have been valid for physical crime – prove to be invalid for many online crimes. The new characteristics of crime – which we discussed in Chapter One – render law enforcement incapable of policing cyberspace. Law enforcement can have limited success in fighting the novice criminals, but determined sophisticated criminals are unlikely to be caught in the net. To remain effective, policing functions must follow a preventive strategy.

Other reasons beside the inadequacy of the law enforcement model in cyberspace can explain the shift to a new paradigm of policing. The reactive policing model was never ideal to begin with, but adopted as the second best option because prevention was far more expensive. The online environment, however, is much better equipped for crime prevention than for law enforcement. It is an environment in which prevention can work fairly well and is relatively cheaper than the cost of online law enforcement.<sup>6</sup>

In a digital environment, various preventive strategies become available. We can design the architecture, the code, to prevent the possibility of certain crimes. Furthermore, with the digitization of operational intelligence, automated tools and effective points of control, preventive policing is optimized. We can program the patterns of crime, identify and then predict in real time the probable incident of crime. Once we are able to predict a probable crime, we can prevent it from happening.

Further, the transition to preventive strategy can be explained institutionally. The online “space” is governed by private entities that strategically prefer to manage their risks than be assisted by law enforcement.

We are still in the process of a paradigm shift. There has been no constitutive moment in which the law enforcement model has been formally abandoned, replaced by the new cyber policing model. It has been a gradual process; more and more the new policing steps that are taken cannot be explained with the old model. They do not correlate to the old method of operation of law enforcement, but rather reflect the logic of the new model. At the time of transition between paradigms, it is common that people are seeking the old and familiar paradigm to explain the new observed reality. Policy makers, who

---

<sup>6</sup> The change in the relative costs of law enforcement versus preventive strategy can be related to two factors: First, law enforcement has become an increasingly costly operation with the growing need for comprehensive forensic examinations of each crime, cross-border operations and multi-sites searches for evidence. Second, preventive strategies were more expensive when they focused on the perpetrator, since it was harder to locate a potential perpetrator and predict the particular crime. The online environment enables the shift to prevention; protecting the potential victim as opposed to chasing after the criminal. Aside from these factors, the assessment of whether it is economically wise to invest in preventive measures is a function of the expectancy of damage. It is also affected by the likelihood of capturing the perpetrator. Prevention is becoming more and more preferable with the decreasing chances of successful online law enforcement and the growing damage expectancy from potential crimes.

are educated to the traditional mindset of law enforcement, call for better law enforcement solutions to tackle cybercrime. They call for harsher punishment, higher budgets for law enforcement and improved investigatory techniques. At the same time, privacy advocates who were acculturated to consider the criminal procedure as the Magna Carta, seek there for better civil liberties' assurances. Yet, the ship has already sailed and both efforts are futile.

This chapter aims to describe the process of this paradigm shift. It will explore how different developments in the law, policing practices and technology have emerged together to form the new paradigm. The professional law enforcement model is a reactive strategy that is enforced through the police. We can track the transformation to the new model on both axes: *strategy* and *organizational structure*.

The professional law enforcement model tends to follow a reactive strategy with certain embedded attributes<sup>7</sup>: 1) ***Criminal focused*** - Focus on the potential criminal it aims to deter; 2) ***Law as primary deterrent*** - Criminal law is the central tool that the formal public system uses for deterring criminal activity<sup>8</sup>; 3) ***Passive victim*** - The victim has no active role in preventing or responding to crime (with the exception of self defense); 4) ***Evidence based investigation*** - An investigation is opened in response to a particular crime and aims to gather incriminating evidence that can be later presented in court; 5) ***Discretionary enforcement*** - Discretion is exercised whether to open or continue an investigation and whether to prosecute; 6) ***Deferred Judicial sanction*** - sanction is imposed by court after convicting a defendant.

---

<sup>7</sup> Not all of the assumptions are equally essential for the reactive strategy of law enforcement. The law enforcement model has developed to normally maintain all of these attributes, but a reactive strategy can be constructed even if we were to relax some of the attributes. In essence, a reactive strategy only implies that we deter a criminal by the likelihood of a sanction, and that we respond to a crime rather than proactively seeking to prevent a crime. Yet, the modern materialization of reactive strategies in democratic societies tends to embody the aforementioned attributes. We normally associate reactive models, which do not embody these attributes, with totalitarian regimes; less emphasis on formal prosecution and judicial sanctioning.

<sup>8</sup> The law enforcement model can still recognize it is not the only deterrent for criminal activity and not even the strongest deterrent. Other deterrents such as social norms, market and architecture also have their role. However, in the traditional law enforcement model, the formal system primarily manipulates the law to achieve deterrence. In other words: law enforcement does not deny the effectiveness of other deterrents, but conceives its formal deterrence to strategically play a specific tool, the law.

There is no single required organizational structure to operate a reactive system of policing. This system has operated at different times in history with various organizational structures, private and public. However, the professional model of law enforcement has become a distinctive mark of modern sovereignty. It controls the use of coercive force within its territory and hands it to a professional public police force.<sup>9</sup> The public monopoly over the use of force traditionally had certain distinct elements: 1) *Territorial* (matches the jurisdiction); 2) *Central command* – to gain control, the structure of policing is relatively central and hierarchal; 3) *Public officials* (meaning no formally assigned policing roles for private parties); 4) *Limitations on the individual use of force*.

As this chapter unfolds we will explore how both the strategy and the organizational structure are challenged in the emerging CyberPolicing Model. To reveal the full picture and see how the paradigm of law enforcement is in the process of collapsing. It would be useful to look at each element of the model and see how it is changing.

I will first explore how the law enforcement model has been gradually restructured offline. The change can be mainly attributed to the rapid growth of the private security industry. This has both challenged the public nature of law enforcement and its dominant reactive strategy. Private security has grown in an environment of decreasing trust in the ability of the law enforcement model to reach satisfying results in contemporary urban society. Private security currently outnumbers the public police, and serves all the functions that heretofore were exclusively controlled by the police. More and more spaces that serve for public interactions are organized around private security control,

---

<sup>9</sup> In most jurisdictions, there is no single organizational structure for law enforcement. Yet, the traditional law enforcement model is, in most western countries, heavily based on public police. Still, there was always a certain degree of non-public policing activity, which was tolerated to different degrees in different jurisdictions. As our discussion unfolds, we will see that there is nothing inherent in policing that requires it to be accomplished through public entities. A reactive policing model can also be operated by private parties which was the historical model. Recently, policing activities are restructured again to focus primarily on private parties. As we will see later, all functions which are traditionally associated with the police are also carried out by private security companies which outnumber the police in most western countries.

from the town mall to the gated communities. Private security strategically favors prevention over detection and punishment. It measures its success in preventing crime and reducing damages of unwanted activity and not by numbers of arrests and convictions (the common measurement for policing performance). It operates by denying access or revoking permissions for usage from unwanted individuals, rather than by sanctions of a formal judicial system.

The growth of the private security industry led to a “search for identity” within the public police as well. The police realized that an exclusive reactive strategy, focused on criminal justice, is not producing the expected results. Therefore, it should be open to alternative strategies. To that end, the public police have been engaged increasingly in various preventive initiatives: designing physical architecture to constrain crime; tackling public disorder which could lead to serious crime; and, most notably, “*community policing*”. The police are willing to share its mandate, and partner with the members of the community, who possess specific localized knowledge that can help prevent crime. The success of all these preventive initiatives is debatable, and they represent only a tiny fraction of current police activities. The police offline is still mainly a public force that responds to committed crimes. However, these initiatives carry a significant importance: they started a process of change in the police mindset and in the self perception of the police activity. This change in mindset set the seeds for the paradigm shift online.

This chapter examines how the paradigm shift is emerging rapidly with the growth of online crime. Online, the dominant paradigm of policing is no longer the law enforcement model. Investigations and prosecution are assigned only a peripheral role in cyberspace.<sup>10</sup> At the core of online policing stands an opposite paradigm, the CyberPolicing, which is a proactive system with a hybrid organizational structure. This

---

<sup>10</sup> Criminal law carries an important role of regulating what is an unaccepted behavior in society. Prosecution of infringement of criminal law serves an educational role and a symbolic function. Law enforcement is no longer the prominent tool in fighting crime, but society still has an interest in prosecuting certain crimes. The police are still called upon to investigate and prosecute certain committed crimes in the online environment, but it is peripheral to the preventive strategy. Having said that, prosecution may have an important role even in a system which is based on crime prevention strategies. We can expect more prosecutions of attempts to commit a crime. However, such prosecutions are no longer part of an overall reactive system.

new model is not yet self-evident. The formal rhetoric and much of the scholarship in the field still adheres to the law enforcement model. One must connect seemingly unrelated developments in the law, policing tools and institutional settings to be able to capture the new structure that is emerging. We need to conduct an experiment that is similar to looking at a three dimensional picture. If you focus on a particular dot in a three dimensional picture, you would just see its shape reflected on the observed surface. However, if you relax your focus and distant yourself from the image, you would be able to see a new complex structure that suddenly emerges. Most of the scholarship in cybercrime is focused on these particular dots. It analyses a particular dot – a particular policing practice or a specific legal doctrine - and tries to understand its role or its implications. It assumes that all the dots are still part of an overall familiar structure, the law enforcement system. When the dot does not fit the existing structure, we often brand it an exception; a minor deviation within the overall system. This chapter encourages us to question our assumptions of the existing structure. To continue the metaphor; this chapter questions whether the dots are actually part of a familiar structure or whether they have emerged into a totally different structure manifesting a much higher level of complexity.

I will follow the dots to see how the new emerging structure is the polar opposite of the current law enforcement system in both its strategy and organizational structure. This new strategy is composed of the following attributes: 1) **Proactive** –acting prior to a commitment of a crime to prevent it. It operates with various proactive tactics: Operational and Predictive Intelligence, Undercover entrapments, Preventive architecture, Operational surveillance, Community policing, and Identity control ; 2) **Intelligence based** – ubiquitous collection and sharing of general operational intelligence which includes; communication content, traffic data and third parties’ collected information. Currently, intelligence is gathered with no particular connection to a specific crime or a specific suspect. 3) **Architecture as a primary tool** – policing strategically employs architecture, the code, as the primary constraint to crime (rather than law as the primary constraint); 4) **Automated, non discretionary** – automated policing replaces human discretion. Simultaneously, enforcement is done through third-parties, such as

Internet service providers, which are required to incorporate policing functions, but are granted no discretion; 5) ***Present non-judicial sanctions*** – these sanctions carry the form of restrictions on access or denial of permissions, and act as a constraint with no judicial decision. Further, alternative sanctions that were long time advocated, such as public shaming, are increasingly gaining dominance online; 6) ***Active victim*** – victims are both empowered to serve in the policing process and also mandated to take certain preventive actions; 7) ***Intermediaries focused*** – the policing operation does not necessarily focus on the perpetrator, but on the intermediaries who can prevent the risk, control it or mitigate it.

The change in strategy is closely connected to the change in the organizational structure. Similar to the offline world, the transition to private security also transforms the strategy. Currently, offline public policing is relatively limited in its strategic flexibility. Its practices are linked to a particular legal structure which controls its power and fixes its operation. Furthermore, the organizational design of public policing is less adaptive to changes in strategy. However, with the growth of private security entities, there is a myriad of possible organizational structures that can be adapted to alternative strategies. In the online environment, the role of private parties increases dramatically. All activities occur within privately managed “spaces”. They become the primary security providers and not a junior partner to public police.

Furthermore, the emerging organizational design does not follow clear dichotomies of private vs. public entities, for-profit vs. not-for-profit, and voluntarily vs. mandatory. There is a complex network of relationships developing between the various private entities (individuals, commercial security companies, service providers, and non-profit groups) and the public police. All of these entities serve a role in the emerging policing structure. However, the role of each entity is not constant in all policing activities. We will explore the complexity and diversity of all the possible relationships between these private entities. In general, the evolving organizational structures follow some clear attributes which, again, are the polar opposite to the professional law enforcement model:

- 1) ***Multiplex organizational structure*** – various forms of private organizational

structures are engaged in policing functions independently or in partnership with the public police; 2) ***Non-Territorial, Internationalized*** – the organization of policing activities no longer follows jurisdiction lines for both private and public entities. In addition, a supra-national structure is evolving. ; 3) ***Decentralized*** – policing activities are being redesigned in a decentralized structure of a network of policing entities to replace central command; 4) ***Delegation of the policing functions*** – policing functions are delegated, by law or by practice, to private entities ; 5) ***Empowerment of the individuals to use force*** – the law expands the rights of private individuals to use coercive force.

The new environment also requires public police to reinvent its role. While one may think that public policing will gradually become irrelevant with the growing importance of private security, this is certainly not the case. Private security can adequately operate their individual risk management and security operations within their controlled space. So it follows that public policing has no relative advantage in managing these micro-policing activities. However, private entities are not suitable for macro-policing. They have no incentive or capability to manage the risk in the overall environment.<sup>11</sup> Policing in the macro sense is a public good that has to be publicly managed. In fact, the virtual environment increases the importance of this public role. With the growing interdependencies and the risk of cascading failures – which we have discussed in Chapter One – the public entity must manage the overall risk. Furthermore, the public entity provides essential services for the private entities in their risk management operation. Efficient risk management requires timely information about new vulnerabilities, new risks and the timely deployment of security solutions. Finally, the public entity often serves the role of information coordinator, vulnerabilities awareness nerve center, and deployment center for security tools. Granted, it is not the traditional image of the police, but this is the new direction for internet public policing.

The paradigm shift which this chapter describes has been left relatively unnoticed by contemporary scholarship. Scholars have often criticized certain elements of the overall

---

<sup>11</sup> Private security has no interest controlling the risks which their activities externalize to the environment. It is a different problem than the one discussed, and it can be solved by various mechanisms that make private entities internalize the overall costs of their operation.

system, but it was mainly a critique which rested on the foundation of the old paradigm. It is time for a different type of scholarship, one that acknowledges the existence of a new paradigm and questions it normatively. The emerging model of policing is certainly more efficient in tackling cybercrime because it is designed with the particular characteristics of cybercrime in mind. If it is structured with due attention for civil liberties, it can also enhance privacy and protect the individuals from the over-intrusive harms of the old law enforcement model.

However, the new model carries potentially alarming consequences. It changes the power structure in society, and if left unbridled, it can distort this balance of power. The new method of policing has immense implications on equality, liberty, individual autonomy and democratic freedoms. We should be aware of the potentially negative consequences of both the new strategy and the new organizational structure. A proactive model requires us to question the desirability of certain predictive patterns and the effect of preventive measures on society. In addition, a model which is operated by private parties presents the risk of unequal and discriminatory policing, and the risk of untamed use of force.

It is time for contemporary society to engage in an open discourse about the ideal policing system. There is nothing deterministic about the emerging shape of the system. It is currently emerging in a relatively unhampered fashion. The law, as we will see in the next chapter, has not kept pace with it. So, it is time that we decide how we want to control and regulate the new policing environment so we can enjoy its benefits and not suffer its harms. I am not aiming to address all the possible regulations of the new policing system. However, I do believe that we should impose certain restrictions on the new policing system. Society should regulate certain uses of predictive patterns. Certain patterns can predict a crime, but their potential for harm is too great to justify their use. In addition, the collection of more intelligence can always benefit preventive policing, but we have to set clear limits. These limits would regulate the legitimate collection of information and the use of such information. Not all information should be available to the public and in particular to the police to collect and to use. Moreover, the use of preventive sanctions must also be regulated. The use of these sanctions, such as access

restriction or permissions denial, carries immense implications for individual autonomy in the online environment. Last, we need to regulate the private use of force. The current dichotomy between regulation of public use and relatively unregulated private use is unjustified. We can not leave private use of force mainly to contractual arrangements, which are supplemented by property regimes and tort claims. The contractual nature of private policing (supported by property rights) erodes long established civil liberties. We must regulate private use of force.

We need to regulate policing, but it must be done with the assumption that policing will follow the new paradigm. Regulations should – and probably would – steer policing in somewhat different directions; as opposed to where it would go if it were unbridled. Depending on the particulars of these new regulations, we are likely to create a variant of the currently emerging system. In essence, however, the police of the future will be a proactive system operated by a multiplex organizational structure. We are not going to return to predominately professional law enforcement system. It is no longer a valid option in the new crime scene. Moreover, it is not the desired system of policing. We must take advantage of the potential of the new environment to produce a better system.

The current chapter will serve us to start the long due normative discussion about the proper regulation of policing operations. In this chapter we set the descriptive foundations for this discussion by portraying the emerging model of policing. The next stage of my project – Chapters Three and Four – will start from the assumption that we will have a new system of policing which will be based on the new paradigm. It will question the appropriate methods to control the operation of such a system. It will also question whether the change in policing paradigm should also change our system of control of policing operation.

---

*[Second excerpt from chapter two – Why new model? p. 99-121]*

### **III. Why is the Professional Law Enforcement Model not followed online?**

The professional law enforcement model has dominated modern societies and has become closely associated with our conception of the nation state. When contemporary society started to experience growth in cybercrime, the natural response was to call for the familiar model of policing to address also the new types of crimes. After all, the reactive strategy had managed to contain criminal activity for millennia, in spite of dramatic changes in the social and technological lifestyles. This model had effectively managed to tackle crime, even when patterns of criminal behavior and criminal organizations changed dramatically. So, what is more natural than the continued reliance on the same model of policing for new types of crime?

Calling for the familiar model of policing to also address cyberspace was indeed the natural and expected response to cybercrime. Regulators, who were accustomed to the idea that criminalizing an act and setting a price for crime deters criminal behavior, were called upon to prohibit these new forms of criminal activity by imposing harsh punishments. Scholars have suggested imposing even harsher punishment for cybercrime; to offset the decrease in apprehension. This diminishing deterrence is the result decreasing costs for committing crime online and perceived reduction in the probability of enforcement.<sup>12</sup> The first wave of cybercrime regulation (Cybercrime Law 1.0)<sup>13</sup> was legislated according to the old and familiar patterns. It was a wave of substantive criminal law regulation: setting new prohibitions to address unwanted behaviors in cyberspace and setting legal penalties to achieve optimal deterrence. The common notion of that time was that we lack the appropriate substantive criminal law (meaning criminal prohibitions) to tackle cybercrime. However, it was more of a myth than an accurate description of the law. Actually, there was very little missing in the

---

<sup>12</sup> Neal Kumar Katyal, Criminal Law in Cyberspace, 149 *University of Pennsylvania Law Review* 1003, 1005-1006 (2001). *[ to cite also others who recommend to have special sentencing considerations for cybercrime]*

<sup>13</sup> I have used in my former work the terms “cybercrime law 1.0”; “cybercrime law 2.0” and “cybercrime law 3.0” to describe the evolution and changing nature of cybercrime law. See: Nimrod Kozlovski, ‘Securitizing’ the Internet – A Socio-Political Analysis, Oxford Internet Institute, Summer Doctoral Programme, July 2004 (at: <http://crypto.stanford.edu/portia/talks/nimrod2004.ppt>).

substantive law. Common definitions of crime were normally broad enough to cover most occurrences of cybercrime.<sup>14</sup>

The first wave of cybercrime law did not prove to be effective. As a matter of fact, cybercrime was constantly growing. Law enforcement officials and scholars then argued that the problem is with procedural law that is not adequate for cybercrime investigations. This is certainly true, since criminal procedure is structured to fit the physical crime scene, and is ill-equipped to handle digital investigations. Scholars have therefore proposed a set of specific criminal procedures for digital investigation.<sup>15</sup> These special procedures are called to address, inter alia, the retention and preservation of digital evidence, the search and seizure of computer and network evidence, electronic surveillance, and admissibility of digital evidence in court. Digital investigation procedures have grown in the last decade to become a distinct and mature body of law. This procedural wave of regulations (Cybercrime Law 2.0) was followed with international agreements. The international agreements – and most notably the European cybercrime convention – were postulated to assure that the substantial regulation (Cybercrime Law 1.0) is adopted into local legislation and that the special procedural mechanisms (Cybercrime 2.0) are implemented across-jurisdictions. These international agreements also established special mechanisms for trans-border law enforcement assistance.

The procedural regulations (Cybercrime Law 2.0) and the international instruments suffer from the same problem as the substantive regulations that preceded them (Cybercrime Law 1.0). They are based on the assumption and application of the professional law

---

<sup>14</sup> While this was true for western countries, even during the first incidents of cybercrimes, it has taken a bit longer for developing and undeveloped countries to amend their laws to capture certain incidents. The case of the I Love You bug, which created worldwide damage, but could not be prosecuted in Philippines because of the absence of criminal probation, served as a common example of the failure of developing countries to catch up with cybercrime. However, this case is an exception, and the progress that was made in computer crimes legislation worldwide, made such an incident less likely to repeat itself. When substantive law does not cover a cyber activity, it is normally an intentional decision not to criminalize such act. This is the case, for example, with hate crimes in the U.S. or individual copyright piracy in other jurisdictions.

<sup>15</sup>Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Columbia Law Review 279 (2005); Nimrod Kozlovski, The Computer and the Legal Proceedings – Electronic Evidence and Court Procedure (Israeli Bar Association, 2000).

enforcement model. They assume that local public law enforcement authorities will react to a committed crime. This is a new body of law, but, again, it rests on the assumption of the familiar law enforcement model.

I have no doubt that the new regulations – primarily the procedural body of law – are essential for the efficient enforcement of cybercrime. However, I do not think that this body of regulations, or any alternative regulations which rests on the assumption of the professional law enforcement model, is likely to solve effectively the problem of cybercrime.

The professional model of law enforcement is no longer a plausible or desirable model of policing. Law enforcement still has a role to play in the cybercrime environment, yet it cannot be the predominant paradigm of policing. Prosecution of cybercrime can and should supply the moral symbol of the law and may deter the insignificant petty criminals. However, it cannot properly handle the sophisticated and determined criminals and is unlikely to contain their considerable potential for damage. Cybercrime will be eventually policed primarily by a proactive model of enforcement that would be operated by a multiplex organizational structure. As we will see later in this chapter, in practice, such a system of policing is already emerging and is replacing the old law enforcement model.

The professional law enforcement model is replaced by a proactive system for three main reasons: 1) The professional law enforcement model assumes deterrence, possibility of successful investigation and manageable damages of disorder– all these assumption are invalid for certain cybercrimes; 2) Prevention becomes economically and technologically more efficient, and potentially less intrusive than law enforcement. It affects the traditional public choice for a second-best reactive system; 3) In the new online environment the Points of Control, meaning the efficient “locations” to detect crime and make policing intervention, have changes. Online, private entities control the points of efficient policing intervention, and they strategically prefer to manage risk with preventive mechanisms, and not be assisted by a reactive law enforcement system.

In the first chapter we investigated the nature of cybercrime and identified unique characteristics of it. We explained why several of these characteristics pose a unique challenge to law enforcement. Each characteristic, to a certain extent, eroded the efficiency of law enforcement. The aggregate effect of these characteristics renders the law enforcement model's assumption invalid altogether. This is normally the time for a paradigm to be abandoned, when its underlying core assumptions prove irrelevant to a changing reality. Let's further develop this argument.

As we mentioned, the law enforcement model rests on three primary assumptions: criminals are deterred by the probability of sanction; investigation is likely to trace the criminals and provide evidence for prosecution, and the damages of disorder are manageable. These aforementioned assumptions may be reasonable for most physical crimes and some cybercrimes.<sup>16</sup> However, these assumptions are not valid for other cybercrimes and for the sophisticated offenders. As the offender can design the crime to take advantage of the unique characteristics of the online environment, the law enforcement model's assumptions are put in question. We saw in the first chapter how the criminal can strategically design the digital crime to be untraceable, unidentifiable, unobservable, unreadable, automated, propagating, distributed, and internationalized. When a crime carries these characteristics – or even a few of them – the law enforcement model can no longer be the primary solution.

Let's start with the assumption of deterrence. According to this assumption, to deter a particular crime, the expected penalty – that is the severity of the punishment, and the probability that it will be imposed – must exceed the gain to the offender. This is an economic theory about human incentives. When the economics indicate that deterrence is implausible, it is time to rethink the strategy.

In economic terms, the problem is that all of the above factors work against the plausibility of online deterrence: First, the criminal can control the severity of the

---

<sup>16</sup> Susan Brenner, *Toward Criminal Law for Cyberspace*, Ibid.

punishment by jurisdiction arbitrage, as we saw in Chapter One. He can either initiate the act from a jurisdiction where it is not a crime, and therefore has zero expected penalty, or shop for a favorable jurisdiction where the punishment is negligible. Second, and more common, the criminal can design the crime so as to reduce the probability that he will be punished. . He can practically stifle the possibility of investigation and prosecution by designing the crime to be unidentifiable, untraceable, unobservable or unreadable. This he can do with the use of technologies introduced in Chapter One; anonymization, untracability, encryption and steganography. As we saw, these tools do not require any sophistication. They are freely available, and can be employed for most crimes. Third, the expected gain for the online criminal distorts the common assumptions about deterrence. Normally, in physical crimes an unsophisticated criminal would gain little from certain crimes (such as theft or financial crimes) and would have a relatively high risk of being caught. This created an effective deterrence for most potential criminals. The system was based on this assumption that crimes are an anomaly to normal behavior because most people have their incentives set ex-ante not to commit a crime.<sup>17</sup>

Online, as we saw in Chapter One, the unsophisticated criminal has a gain expectancy that is disproportional to his skills. This is due to automation and propagation of the crime. Furthermore, the expected gain is also a function of the cost of committing crimes. Automation, modularity and digitization lead to substantial reduction in these costs. Add that to the reduced probability of getting caught, and it is easy to understand why crime pays in cyberspace.

Last, offenders who seek destruction may not follow the normal expected deterrence pattern. Just as penalty is not expected to deter a suicide bomber who is willing to sacrifice his own life, so may be case with a “virtual terrorist”. The internet, as we saw in Chapter One, provides an attractive platform for offenders that are motivated primarily for destruction. Control-by-deterrence is obviously an improper strategy for these offenders.

---

<sup>17</sup> When we say that the system is reactive, we mean that the law enforcement response goes into operation after the crime is committed. Yet, the assumption of the system is that, most of the time; we will not need a response because people will be deterred from committing them.

The assumption of deterrence embeds another assumption; that an investigation of the committed crime can secure evidence for future prosecution. With no evidence, there is no punishment. This assumption of deterrence deserves a closer look - as it seems fundamental to the failure of the law enforcement model. The criminal can employ different strategies to stifle the investigation or to render it economically infeasible. He can make the crime itself unobservable, and therefore stifle detection that would lead to investigation. Further, he can make the evidence unobservable (steganography) or unreadable (encryption) and stifle or complicate an investigation. Alternatively, he can create a smoke screen – as we discussed in Chapter One – that would make him undistinguishable from an army of zombies, all seem equally suspicious. Moreover, he can commit his acts in an untraceable manner, employing one of the tools, discussed earlier, and stifle attribution of the crime. When the actor is anonymous and untraceable, he is unlikely to be held accountable for his acts. Last, he can design the crime to have international elements or series of “Hops” between himself and the crime. This makes investigations substantially more expensive and ever dependent on the weakest link in the chain that might not preserved evidence. Since these criminal alternative design options are all freely and easily available, investigations face a tough road. When the technology blocks an investigation – such as with strong encryption of untraceable communication – no resources or extra manpower can save it. Even when the investigation is still possible, the added complexity and costs for each investigation, makes this option impractical.

The problem with transferring the law enforcement model to cyberspace is rooted in the physical orientation of this model. The physical environment follows certain assumptions about the scale, frequency and affect of crime that do not apply online. As Professor Brenner explains law enforcement is a viable option offline (but not online) because it assumes that “crimes will be committed on a manageable scale”.<sup>18</sup> Offline law enforcement assumes that the absolute numbers of committed crimes is relatively low, and that the limited resources of investigation and prosecution will suffice. It also rests on

---

<sup>18</sup> Susan Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 *Boston University Journal of Science and Technology Law* 1, 50-51, 66-68 (2004).

the assumption that real-world crime is “serial crime”. During the event, the offline actor has to focus all of his attention on the victim. . It is only when he completes one crime that he can move on to another. “The one-to-one character of real-world crime derives from the constraints physical reality imposes upon human activity.” This assumption is no longer valid with the automation of crime: “Automated crime is using the technology to multiply the number of ‘crimes’ someone can commit in a given period to time; automation gives perpetrators the ability to commit many cybercrimes very quickly”. While automation increases immensely the number of committed crimes, investigation and prosecution are, in essence, still a serial operation. Law enforcement needs to detect, investigate and prove in court each individual crime separately. Law enforcement’s limited resources are no longer adequate to deal with the scale of crimes in society.

Facing all of the abovementioned obstacles, digital investigations are unlikely to catch the savvy criminals. Investigations may catch the unsophisticated criminals and deter them, but this is not going to solve cybercrime. Researchers indicate that in order to tackle many types of cybercrime, law enforcement needs to get to the sophisticated players (the “hubs”) while the petty criminals (the “nodes”) are meaningless.<sup>19</sup> In cybercrime, prosecuting the petty criminals is shown to not only have no positive deterrent on the sophisticated criminals; it may even do the opposite. Since the investigatory and prosecutorial resources are being exhausted to chase petty criminals, fewer resources can be devoted to trace the sophisticated criminals.<sup>20</sup> It was common in offline investigations to use the petty criminals to get to the big fishes whom they collaborate with or work for. However, as our discussion in Chapter One indicates, this is unlikely to work with online forms of collaboration. Normally, collaboration happens without direct interaction or even an encounter between the collaborators. The same holds true even with certain hierarchal structures of online crime, where “soldiers” often do not know their operators. Take the script kiddies, for example, who run automated

---

<sup>19</sup> *[To add citations for the network analysis of crime control and for the change from thinking about the nodes to thinking about the hubs]*

<sup>20</sup> The distorted structure of incentives in the current policing system even exacerbates this problem. Policing success is measured by the number of arrest and convictions. These measurements create an incentive for the police to catch many petty criminals, who are easier to track and prosecute, then to conduct complex investigations which aim at the roots of the problem but have uncertain success chances.

scripts for DDoS or hacking systems. They may use the sophisticated tools developed by a few sophisticated hackers, but they normally have no information that can lead the investigator to the source.

Last, the assumption about bearable damages is no longer valid online. Offline, the reactive strategy can provide a fair solution for crime, since that damage is normally bearable. Even if the crime has devastating consequences for the particular victim, for society at large, the damage is still bearable. Society can decide to internalize the costs of that crime, rather than invest in a better policing system. This decision assumes the particular conditions of physical crime: the absolute number of crimes is limited; the damage of each crime is confined; and, the exploitation of vulnerability of a particular victim is separated from the exploitation of other potential victims. Our discussion in Chapter One, about automation and propagation, teaches us that these conditions are not valid for certain cybercrimes. We saw that some of these crimes are automated, and therefore the number of crimes or their potential damage, is no longer correlated to the number of criminals. This asymmetric threat changes the criminal landscape. Further, crime tends to propagate creating damage that is not confined to any particular location. Moreover, with an increasingly interconnected environment and with the risk of cascading failures, the potential damage to society may just be of an unbearable magnitude.

When risk follows the abovementioned patterns, a deferred law enforcement reaction to crime is inadequate. Even if we assume a successful law enforcement reaction to a particular crime, it would not often be a sufficient solution. One of the assumptions of the law enforcement model is that, once the offender is caught, further damage is prevented. Once the offender submits to the authority of the police, he is assumed to stop offending. If he is also prosecuted and imprisoned, he cannot further offend while he is in custody. This assumption has often been proved wrong for certain cybercrimes. Since the crime is automated, the damaging effect can continue, even if the offender is caught. This was the case, for example, with an employee who was arrested, but at the same time a hidden “logic bomb” he installed at his employer’s computer, was set to destroy the system.

Additionally, since the crime is already propagating, it can continue its effect even if the originator voluntarily submits to authority or seeks to stop it. Once the attack tool is unleashed or an illegal file is distributed, it is often outside the control of the originator to stop the damage or even mitigate that effect. Such was the famous case of Morris, who developed one of the first worms. He did not expect the potential for propagation of his experimental software. While he was trying to stop it from propagating and while he was cooperating with the investigators, he lost control of it.

Cybercrime scholars have long argued that the conditions of cybercrime are different from physical crime. These scholars have focused on various attributes of cybercrime that make the current policing system incapable of dealing with it. They have identified certain characteristics of cybercrime in particular – mainly unreadability (encrypted information) and anonymity - as fatal to law enforcement efforts. Accordingly, scholars and policy makers have suggested specific solutions to tackle these particular attributes through legislation or a specific technical mandate. To tackle the challenges posed by encryption, for example, proposals were considered that would ban certain uses of encryption, limit its export, and establish a key escrow regime to retrieve encryption keys, or mandate a back door to encryption software. All these proposals may alleviate, to certain extent, a particular problem in policing cybercrime, but can not be the ultimate solution to cybercrime.

Cybercrime is a unique challenge for policing. There is no magical solution that can address effectively all attributes of cybercrime that complicate law enforcement. It is the aggregate effect of all the different attributes that makes cybercrime a crime of a different nature, which can longer be addressed properly by the law enforcement model. As our discussion has revealed, these new characteristics render law enforcement assumptions invalid and obsolete. This has led policy makers and scholars, most notably Susan Brenner<sup>21</sup>, David Johnson, John Palfery and Susan Crawford<sup>22</sup>, to call for various alternative models of policing.

---

<sup>21</sup> While I strongly agree with Professor Brenner's argument that the law enforcement model is rested on assumptions that are no longer valid, I do not share her view about the alternative system of policing. In a

We can explain the abandonment of the professional law enforcement model with an analysis that is *internal* to this model. This is the aforementioned analysis of the law enforcement's model invalid assumptions in cyberspace. But, we can also explain the abandonment of the law enforcement model in *comparative analysis* against a proactive model. A reactive policing model was never the ideal, but a second best option, adapted mainly due to the cost of an alternative preventive solution. Leaving aside for now the normative question of whether there are reasons to prefer a reactive or a proactive system, it is safe to assume, that given the choice, society would prefer a solution that can prevent crime from happening in the first place. The main considerations to not shift to a preventive system have been cost, invasion of privacy, and the problem of over prevention of lawful activities. We tend to believe that proactive model is inferior to reactive model in all of these three aspects. This may be true for physical crime, and therefore we can understand society's choice to implement a primarily reactive model. However, the shift to cyberspace has transformed all of these aspects; cost, privacy and over prevention. We will further develop this argument when we analyze the practical policing methods that are implemented online. We will also see how proactive models can be employed with relatively low cost, a potentially minimal invasion of privacy and a potentially low ratio of prevention (false positive). At this stage, however, we will discuss why the comparison between reactive and preventive models may lead to other conclusions in cyberspace, and therefore further encourage the shift to the preventive model.

---

nut shell, professor Brenner offers to establish a system of incentives for distributed security which is largely focused on the victim's defensive security tools. She aims to create incentives for victims so that they do not remain passive, waiting for a central response. In essence, this suggestion is similar to Alon Harel's and Omri Ben-Shahar's suggestion to establish a principle of *contributory fault* which was mentioned earlier (see: footnote \_\_\_). Brenner's suggestions further develops this idea and adapts it to the particular circumstances of online distributed attacks, discussed in Chapter One (for similar proposal see: Brain C. Lewis, Prevention of Computer Crime Amidst International Anarchy, 41 American Criminal Law Review 1353 (2004)). However, Brenner's suggestion still rests on the basic assumption of primarily reactive public law enforcement system. She offers to prioritize enforcement based on the victim's investment in defensive mechanisms and to also outlaw victimization which facilitates further crimes (the Zombies scenario). This all assumes a policeman, an investigation and a public criminal process in which the victim's behavior is taken into account. This may be an improvement to the current deterrence system which almost always ignores the victim's behavior even if his investment in some defense would be socially optimal. However, as a solution which rests on the law enforcement model, it cannot be the primary solution for cybercrime.

<sup>22</sup> David Johnson, Susan Crawford & John Palfery, The accountable Net – Peer Production of Internet Governance, P Virginia Journal of Law & Technology 9 (Summer Issue, 2004).

Cost has always been the main constraint for society to shift to a proactive system. Offline, it is much more costly to keep order and prevent crime than to respond to a limited number of committed crimes. This is assuming that most people are deterred ex-ante from committing a crime. Public prevention of physical crime has proven to be very costly and has a limited effect (unless the community is participating in its own policing).<sup>23</sup> The digital environment has changed both the costs and the expected gain. Prevention has become cheaper and more effective. At the same time, as our former discussion indicated, the cost of law enforcement is increasing significantly, while its efficiency is decreasing.<sup>24</sup> In a digital environment, various preventive strategies become available and relatively cheap to employ. Prevention can operate in many strategies such as: designing the software and hardware (“Code”) to prevent the commission of crime; gathering operational intelligence; or, monitoring traffic to identify patterns of potential crime and thus prevent it in real-time. We will later discuss in details all these and other proactive tactics.

---

<sup>23</sup> To prevent crime at its roots requires major investments in education and social welfare that the modern capitalistic state is unwilling to spend. Alternatively, we can design the physical architecture to reduce the opportunities for some crimes, but it requires large investments and major changes to existing architecture. Therefore, society has mainly considered prevention methods that are based on operational intelligence or visible policing presence. Both methods are very expensive. Just to get an idea, figures teach us that to add a single patrolling policeman to the street for a full day, takes 10 overall additional positions to the police force in an estimated annual cost of 500,000\$. Furthermore, research has shown that an increase in the number of patrolling policeman may only have marginal contribution to the reduction of crime. The most important factor in crime prevention is access to local knowledge which the police often lack. For these reasons, as will see later, preventive policing has shifted offline to collaborative projects with the local communities.

<sup>24</sup> The change in relative costs of law enforcement versus preventive strategy can be explained in two ways: First, law enforcement has become an increasingly costly operation with the growing need for comprehensive forensic examinations for each crime, cross-border operations and multi-sites searches for evidence. Second, preventive strategies were previously costlier to operate when they focused on the perpetrator, since it was harder to locate a potential perpetrator and predict the particular crime. Preventive strategies can be easier and cheaper to operate at the victim’s end. The online environment enables us to shift the location of preventive measures from the perpetrator’s end to the victim’s end. Aside from these factors, the assessment of whether it is economically wise to invest in preventive measures, is mainly a function of the expectancy of damage. It is also affected by the likelihood of capturing the perpetrator who will be charged to pay the damage. Prevention became growingly preferable with the decreasing chance of successful law enforcement and the growing damage expectancy from a potential crime.

When the code is designed to prevent crime, it is no longer a matter of choice whether to commit a crime, because the option or opportunity for criminal behavior is removed.<sup>25</sup> If the code is designed to prevent crime, and assuming that it is not circumvented, there are no further costs for policing. The code polices the user.

Alternatively, with the use of automated tools, gathering operational intelligence becomes cheap. Since the collected data is digitized, making use of it becomes even cheaper. It does not take the same manpower and resources to collect and analyze intelligence as it did offline. We can automate this process and tell the computer what to collect, what to look for, and when to alert a human operator. Moreover, criminal intelligence investigations charged with studying organizational structures<sup>26</sup> that were traditionally very expensive and consumed immense manpower can now be automated and cheap to operate. Automated network analysis tools can automatically analyze and visualize the organizational and operational structure based on communication patterns (with no access to content). Furthermore, useful operational intelligence can be collected in cheap and automated undercover operations. Undercover operations were too costly and too risky to employ in physical space. They were also selectively employed, since the officers were “burned out” after their identity was disclosed.<sup>27</sup> Online honeypots (automated traps) and automated agents (“bot Cops”) are relatively cheap, require limited if any manpower to operate, and are practically risk free. They can effectively acquire precise operations intelligence.

Last, if the policing function (public or private) is positioned in a Point of Control in the data flow, sophisticated prevention tools can operate in real-time. The policing function doesn’t need operational intelligence about a potential target, but can identify and stop in real-time an illegal activity. These digital tools can compare real-time flowing traffic

---

<sup>25</sup> Lee Tien, Architectural Regulation and the Evolution of Social Norms, *International Journal of Communications Law & Policy*, Issue 9 – Special Issue on CyberCrime, Autumn 2004.

<sup>26</sup> Such investigation is set to “determine the size and composition of the group involved, its geographic dimensions, its past acts and intended criminal goals and its capacity for harm” (the Attorney General Investigations Guidelines).

<sup>27</sup> See the Attorney General Guidelines for the Undercover operations which identify the considerations in approving undercover operation.

against recognized patterns of illegal activity or identify anomalies against normal expected behavior. We will discuss how all of these tools operate later in the chapter.

When cost is no longer a constraint for proactive policing, the societal debate shifts its focus to the invasion of privacy and the potential over-prevention of lawful acts. I do not intend in this project to exhaust the discussion on whether these considerations should normatively lead us to prefer reactive system.<sup>28</sup> However, it is important to indicate that, from a civil liberties perspective, the common preference for a reactive system may no longer hold. In physical policing, objections to preventive methods focus on their potential for massive invasion of privacy. These objections are centered around the gathering operational intelligence and the infringement of individual liberty. On the other hand, we normally conceive of law enforcement's deferred response as a limited, proportional invasion of privacy. This occurs only when a crime is committed or attempted, and therefore also does not interfere with lawful acts. There are indications that this may not be the case in cyberspace policing.

To begin with, technological developments have the potential to operate proactively with minimal invasion of privacy. Digital information can be collected, and analyzed without being personally identifiable. This can happen with no possible access to human inspection<sup>29</sup> unless a pre-determined criteria is met (the criteria itself can be democratically decided). Ample of technological tools can protect privacy:

---

<sup>28</sup> I intentionally decided to focus on the description of the paradigm shift which is emerging rather than to engage in an abstract discussion of normative considerations. Such a discussion is essential for contemporary society, but it must be conducted against the backdrop of existing technologies and the reality of contemporary policing. This chapter aims first of all to supply the descriptive background which is missing in contemporary discussion. However, since the professional law enforcement model is no longer a valid option for primary policing model, society will have no choice but to employ various proactive components. The second half of my dissertation will aim to set the structure for the regulation of such a policing system.

<sup>29</sup> The element of human intelligence gathering and analysis versus automated collection and analysis of information has been central in the normative debate about the privacy implications of the new technologies. According to certain notions of privacy, there is no invasion of privacy (or lesser invasion) when there is no human intervention and policing is automated to collect information and analyze it, but not to report to human inspection unless certain conditions are met. This claim seems even stronger when information is inspected automatically according to publicly agreed criteria but no information is collected unless a pre-defined criterion is met.

*Anonymization* of data, *Permission Rules* that are built into the data, and *Access Regulation*. These technologies can substantially change certain assumptions that were valid about the gathering and analysis of operational intelligence in analog format. The works of Kim Taipale<sup>30</sup>, the Markle foundation task force<sup>31</sup>, James Dempsey, and Paul Rosenzweig<sup>32</sup> were groundbreaking in exploring the potential of ***Privacy Preserving Technologies***.<sup>33</sup> Society is given the choice to operate preventive policing, while simultaneously being assured that the policing tools incorporate strong protection of privacy.<sup>34</sup> Furthermore, many proactive real-time policing technologies operate without need for prior information about the individual user. Since the technology can, in real-time, recognize a pattern of potential criminal activity, it can also block traffic (or subject it to other procedure, such as further inspection) based on the type of communication. Spam control, illegal content filters, anti-virus software, intrusion detection tools – all operate based on this method.

At the same time, there are growing indications of severe invasion of privacy while employing the reactive policing model. Cybercrime investigations are leading to an increasing erosion of long standing privacy protections so as to enable investigations. Law enforcement demands new procedures and more invasive technologies to compensate for the growing difficulties in conducting investigations. Indeed, if the

---

<sup>30</sup> Kim A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, *Yale Journal of Law & Technology*, Vol. 7, December 2004; Kim A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 *Columbia Science and Technology Law Review* (2003).

<sup>31</sup> Markle Foundation, *Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force* (2003); Markle Foundation, *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force* (2002).

<sup>32</sup> James X. Dempsey & Paul Rosenzweig, *Technologies that Can Protect Privacy as Information is Shared to Combat Terror*, *The Heritage Foundation Legal Memorandum No. 11*, May 26, 2004.

<sup>33</sup> Their work has been primarily focused on the use of preventive technologies for combating terror. There is still an open debate whether these technologies can be useful in fighting or predicting terror. However, the privacy protection technologies that are suggested in their work is also valuable for policing tools that aim at preventing regular crime.

<sup>34</sup> We must remember however that employing operational intelligence can be very intrusive if such privacy protection measures are not embedded in the policing technology. Only if we insist that operational intelligence technologies are not operated without these features, we can expect them to be embedded in policing technologies. With the appropriate accountability mechanisms that we will discuss in Chapter Four, we can assure that the privacy enhancing technologies were embedded in the design of the policing tool and were practically enabled in actual policing operations.

reactive law enforcement response is limited mainly to the time after a crime was attempted or committed; there are good reasons to believe that evidence will not be available. The criminal, as our previous discussion indicates, can design the crime to stifle deferred investigation. Furthermore, we can expect the criminal to erase direct evidence of the crime that could be found in his possession. Therefore law enforcement is requesting broader authorities in various fronts: 1) Routine mandatory retention of data by intermediaries (mainly ISPs), to assure availability of evidence for potential investigations; 2) Expanded authority to demand various types of data from the intermediaries with or without the suspect's knowledge; 3) Broad warrants to search and seize suspect's computer to enable forensic investigations to find direct or indirect information that he may have tried to hide; 4) Ever increasing authority to employ intrusive surveillance technologies to collect evidence for the crime or to help crack the privacy protection technologies that the criminal used (e.g. Keystroke logger). All these requested authorities are supported by solid logic, and unlikely to be denied from a policing system that operates in a reactive model. The overall result, however, is an immensely intrusive policing system that employs rough tools with major privacy implications.

It is expected that society will gradually refuse to pay the "privacy price" of the reactive system, mainly when there are increasing indications that it can produce only limited policing results. Society will begin to prefer preventive policing and will set the demands for privacy protection measures in the technologies. Furthermore, democratic societies will set guidelines for what information is legal to collect and in what format, what analysis of collected information is permitted, and under what circumstance police will be allowed access to the information and in what format (e.g. encrypted, anonymized or plain text).

The shift to preventive policing also has to face the claim that it is likely to prevent many lawful activities. The reactive model was traditionally preferred because of the assumption that it limited the scope of policing only to criminal activities. The police in liberal society are supposed to stay hands off lawful activities and take action only when

there are reasonable indications that a criminal activity has occurred or will occur.<sup>35</sup>

Therefore, many have objected to preventive policing that by its nature carries a potential to interfere with lawful activities. We need to check whether this assumption is still valid online.

Cybercrime proactive policing is based heavily on predictive patterns. The pattern of criminal behavior is decomposed into elements and then coded. Then the observed behavior or gathered intelligence is compared to the coded pattern. Based on statistical analysis, the system can predict how likely it is that the existence of certain variables in observed behavior, can indicate a crime. Normally the answer will be in a form of a score that correlates to a certain probability. In essence, the system is engaging in the same activity that the policeman employs in deciding whether to investigate a suspicious activity. It is comparing a recognized pattern to an observed reality. This is the nature of the human cognitive process which serves a patrolling policeman in deciding whether a strange activity in the street is the beginning of a crime, or not. Research has repeatedly shown that human intuition often gets the statistics wrong, mainly due to prejudices and stereotypes. Computers are better at identifying a known pattern, if they are coded to search for it, and if the information is presented in the right form. For many activities, computerized pattern recognition can certainly improve policing.

Many still object to computerized predictions, but not because they are likely to do a bad job in recognizing a pattern. The objection is based mainly on three fears: over efficient policing; undesirable patterns or non significant patterns. All these objections are valid, but can be accommodated in the regulation of a proactive policing system. We can decide that even if a pattern is efficient in preventing crime, we do not want it to be too efficient. The price on liberty is not worth paying. We can further decide that a certain pattern, even if it has been proven statistically to predict a high probability of crime, still conflicts with some other value, and we will not allow it. We already do it now with restricting racial profiling. This may have some predictive value, but it is morally

---

<sup>35</sup> Such restricted form of policing has never been an accurate description of reality, but more a libertarian aspiration that informed liberal societies.

objectionable. Last, we can decide that a certain pattern is just not statistically significant enough to predict a crime, so we would not use it. We can set a statistical bar for each type of crime.

Moreover, the use of predictive policing can be done in a sensitive manner. Kim Taipale has noted that the result of identifying a pattern does not necessarily have to be blocking or inhibiting a lawful activity. There may be a menu of different consequences for recognizing each pattern. We can use the pattern recognition only to alert the police that will then follow from there. We can use pattern recognition to further demand an additional security mechanism; such as special code or identification, to better assess the risk. The recognition of a pattern can serve also as a preliminary stage before deciding to increase monitoring. This can therefore potentially increase deterrence and the chances of detection. Furthermore, if the policing activity responds more and more to pattern recognition and at the same time becomes more transparent to the suspect, we have less to worry about. The individual who is notified that he has been flagged by a certain pattern (even without revealing what was the pattern) can then have the chance to explain what his intended activity was and may be allowed to proceed with it.

We should also acknowledge that there is an increased risk of prevention of lawful activities in the law enforcement based model. An increasingly intrusive law enforcement model leads to a chilling effect.<sup>36</sup> People self-censor themselves from a lawful activity, because they are afraid that their activity might be later interpreted wrongly and lead to a preliminary inquiry or a full criminal investigation. When law enforcement increasingly uses the new authorities, that we have discussed, this fear increases. Individuals may be reluctant to conduct certain activities and engage in certain interactions, since those

---

<sup>36</sup> “The chilling effect primarily involves the concern that potential lawful behavior, particularly constitutionally protected activity, would be inhibited due to the potential for a kind of post hoc surveillance (“dataveillance”) that may result from the increased sharing of information among currently discrete sources. ‘Potential knowledge is present power’, and awareness that government may analyze activity is likely to alter behavior, ‘people act differently if they know their conduct could be observed.’ The risk is that protected rights of expression, protest, association, and political participation may be affected by encouraging conformity, discouraging dissent, or otherwise alerting participation in political life.”, Kim A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, *Yale Journal of Law & Technology*, Vol. 7, December 2004.

actions could be interpreted out of context, or be used to formulate an investigation based on a mistaken hypothesis.<sup>37</sup> As information usage becomes less and less within the control of the potential suspect, and law enforcement gathers information from third parties, possibly without his knowledge, such defensive behavior is more likely. The fear of Kafkaian scenarios can restrain many lawful activities.

We can conclude this part of the discussion by saying that the assumptions about cost, the invasion of privacy, and over prevention that were valid for offline policing, may change in cyberspace. The societal preference for reactive policing is likely to change with the decreasing cost of preventive policing. Furthermore, assumptions about relative civil libertarian preferences for reactive policing may change as well. The law enforcement, reactive policing system in cyberspace becomes more intrusive and further leads to increasing self censorship. At the same time, while preventive policing may pose immense dangers to privacy and liberty, there are technological solutions and policies that can protect it. These new privacy protecting technologies offer society an opportunity to regulate the use of policing technologies, while demanding protective features and adequate policies for their use. Therefore, we can expect society to gradually set a preference for preventive policing technologies. The normative preference for preventive technologies will further support the transition from the reactive model which has been proven to be incompetent, to properly police cyberspace.

---

<sup>37</sup> Professor Helen Nissenbaum emphasizes in her research the importance of Contextual Integrity for information privacy, see: Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 *Washington Law Review* 1 (2004). Jason Young recently argued, that the principle of contextual integrity that governs data collection by private entities through fair information practices, should be applied also to data collection that serves for policing purposes. Individual are chilled from lawful activities as they are fearful of out-of-context use of their information. He argued that the individual should have the right to hand information to service providers for commercial purposes, but be protected, to certain extent, from handing this information to the government. The individual should have the right to assert commercial-only context of use, see: Jason Young, *Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation*, *International Journal of Communications Law & Policy*, Issue 9 – Part II, Special Issue on Cybercrime, 2004.

An additional reason why the reactive law enforcement model does not transform to cyberspace has to do with the organizational setting of the new “space”. The change in the nature of spaces and ownership of spaces for public interactions logically leads to privatization of policing functions. Private entities have increasingly greater control over the points of efficient policing intervention. They strategically prefer to manage risk with preventive mechanisms than to be assisted with a reactive law enforcement system.

The growth of private policing in the physical world is often associated with the rise of “*mass private property*”. These properties are owned and managed by private entities, but offer facilities for public access and use, such as shopping malls, education campuses, cinemas, and sport complexes. Shearing and Stenning have researched the growth of these “mass private properties” in contemporary society with the rise of private policing.<sup>38</sup> They found that “private policing grows as the proportion of private landholding accessible to the public grows”.<sup>39</sup> In an environment of expanding growing liability for property owners, the owners of the “mass private property” have strong incentives to provide their own security. They organize their own policing functions to protect from legal liability, and to follow the requirements of their insurance policy. Private policing in these properties is focused on managing risk for the owner of the space. They prefer to prevent the potential of disorder than to assign blame. They often have the reverse incentive structure than the public police, since arrests and convictions are considered as indications of a failure to detect potential disorder and prevent it.

Private policing has expanded to other property arrangements of spaces that are selectively accessible to the public, such as gated communities and commercial districts. These developments shift the responsibility for security in spaces of public use from the government to private security companies. “By blurring the distinction between the public and the private, mass private property attenuates and marginalizes government’s

---

<sup>38</sup> Clifford D. Shearing & Phillip C. Stenning, *Modern Private Security: Its Growth and Implications*, in *Crime and Justice: An Annual Review of Research*, Vol. 3 (editors: Michael Tonry & Norval Morris) (University of Chicago Press, 1981); Clifford D. Shearing & Philip Stenning, *Private Security: Implications for Social Control*, 30 *Social Problems* 493 (1983).

<sup>39</sup> David H. Bayley & Clifford D. Shearing, *The New Structure of Policing – Description, Conceptualization and Research Agenda*, National Institute of Justice, Research Report (July 2001) 23

responsibility for security. It constricts government effort at preventive policing to clearly public venues.”<sup>40</sup> Still, a substantial portion of physical public interactions are conducted in publicly owned spaces, such as the street, the sidewalk, and the public park. In these offline public spaces, the public police are the main provider of policing functions.

The “new spaces” in cyberspace organize in a unique way.<sup>41</sup> The new environment is composed mainly of privately owned “spaces” that are accessible to the public in varying degrees. The virtual “mass private properties” have expanded in scope and their functions to cover many more activities than their physical equivalents.<sup>42</sup> Privately owned sites facilitate a “virtual marketplace”, “virtual mall”, and “virtual sports resort” and many more functions. In the new environment, communities are formed and operate within privately owned spaces.<sup>43</sup> Furthermore, in cyberspace, public discourse is often conducted in privately managed environments. Private entities have become the central provider of services available to the public. At the same time, the equivalent of the publicly owned spaces and commons for public interactions are diminishing in size and importance.<sup>44</sup> Moreover, the infrastructure of public streets and highways of the physical space has not been replicated in cyberspace. The infrastructure for transportation (of data

---

<sup>40</sup> David H. Bayley & Clifford D. Shearing, *The Future of Policing*, 30 *Law and Society Review* 585, 601 (1996)

<sup>41</sup> Much has been written about the problematic use of the space metaphor for “cyberspace”. In essence, there is “no there, there”, there is no space at all in cyberspace. It is only a network that connects networks of computers. It is true that applying the physical spatial logic to the internet is mistaken, since the new environment does not follow the same “physics”. Still, the new environment, the Internet, develops its own geography, its own zoning and new design arrangements which are centered around sites, “virtual gateways” and “virtual locations”. We can say that there is no space in the old and familiar notion, but certainly a new type of “space” has developed. In the absence of an alternative and better metaphor to address the new environment, I will follow the “spatial” terms, but will try to be aware of the difference between the physical space and the “new space” when relevant.

<sup>42</sup> Researchers have studied the growth of the new ‘virtual mass private properties’ and indicated that these new “spaces” have gradually developed to serve more than the common shopping and entertainment functions of the physical “mass private properties”. The new privately managed “spaces” are increasingly becoming an alternative “virtual world”. The owners and developers of these new worlds are nicknamed “Gods” and they dictate the constraints and the “rules of nature” in these new environment. A fascinating series of conferences at New York Law School addressed the growth of these virtual worlds and the role of private entities in their governance (See: *New York Law School Law Reviews*, *The Institute for Information Law Policy Symposium, Special Issue on State of the Play*, 2004).

<sup>43</sup> [Sal Humprhey, \_\_; and \_\_\_\_]

<sup>44</sup> Noah D. Katz: *Sidewalks in Cyberspace – Making Space for Public Forum in the Electronic Environment*, *Harvard Journal of Law & Technology*, Vol. 12 Number 11 (Fall 1998).

packets) is mostly privately held and managed. The control, of both the flow of traffic and the actions in the virtual sites, is, again, privately managed. These entities manage the points of efficient policing in this new environment.

The change in control over infrastructure and spaces that facilitate public functions affect the nature of policing itself. When private entities are responsible for policing and provide private security services, they prefer a different strategy. Like the owners of “mass private property”, owners of virtual spaces prefer to manage their risk, rather than assist law enforcement in prosecuting criminals. They conceive the risk of criminal activity as just another type of risk – as market and natural disaster risks - that their operation needs to take into account. They conduct risk assessment and buy insurance and assign security functions – both defensive and preventive – that can optimally address it.<sup>45</sup> The private entity’s interest may, at times, converge with law enforcement, when he assesses that prosecuting a specific crime serves his bottom line and creates deterrence from further victimizing his business. However, in most cases, private entities conceive their own interests differently than law enforcement. Investigation of a crime can interfere with their business operation, might disrupt business continuity, and often consumes vast internal resources. More importantly, criminal investigation can, and often does, damage the business’s reputation and shares’ value, creates “bad publicity”, and can also lead to civil suits against the company for security failures. Furthermore, surveys indicate that businesses are afraid of the advantage that their competitors can gain during litigation, with the possible exposure of trade secrets in the criminal process.

Private security has never enthusiastically assisted law enforcement in pursuing criminal investigations, and it seems that the new environment has even increased this reluctance. In physical space, the process of criminal investigation was often not in their control. Many crimes expanded beyond their property boundaries, and they were often requested to assist with an investigation that they had not initiated. Alternatively, someone would report a crime that happened on their premises, and they would need to assist law enforcement. Furthermore, the private entity has been cautious in using physical force

---

<sup>45</sup> David A. Skalansky, *The Private Police*, 46 *UCLA Law Review* 1165 (1999).

against offenders, and therefore often needed the assistance of the police. In cyberspace, conditions have changed. The crime is not visible and the private entity would often be the only witness of its own victimization. The crime would start and end at his site.

Therefore the detection of the crime is dependent upon his decision to report it. Statistics indicate that private entities rarely report a cybercrime, and when they do, it is because they are forced to do so by the other victims. Furthermore, private entities are not afraid to use “virtual force” (unlike physical force) and to take actions to address the crime.<sup>46</sup>

They do not need the police to prevent a user from accessing their site, or block a criminal’s traffic. The public police have no relative advantage or even access to the necessary points of control to impose “virtual force”. Last, in order to gain useful information, private entities often prefer to monitor and analyze their offenders, rather than hand them over to the police. For the private party, a monitored offender can be a valuable intelligence source that they do not want to compromise with prosecution.<sup>47</sup>

To conclude this discussion: the shift to private policing also changes the dominant policing strategy. In cyberspace, more than in physical space, private entities have strong interest in assessing their own risks and preventing crime. They vastly prefer this, rather than assisting law enforcement in investigating and prosecuting crimes.

---

<sup>46</sup> Internet service providers are immune from liability for actions taken to filter content and users. A particular legal structure was set to create incentives for them to offer filtering and “policing” services. The law on the one hand does not require them to conduct filtering or policing, and they are not liable for content originated from third parties. On the other hand, the legislator wanted to create a market for added-value services, such as specific filtering and blocking, and therefore render them immune from liability for a decision to filter particular content. Later, we will further discuss the differences between the American and the European regulation of service providers, and the incentives that the regulation creates.

<sup>47</sup> Often companies are afraid of their competitors spying operation, or insider crimes and want to monitor potential attacks to analyze who may be behind them. Companies would normally do that with honeypots that I will discuss later, or in quarantined sites that are not connected to their operational system. With a honeypot, for example, the company can monitor the actions of an attacker; who does not know that he is attempting to hack into a fake system. They can further implant fake documents that seem attractive to potential offenders (e.g. documents that seem to contain trade secrets). They can use digital fingerprints to mark the fake document and then to track its whereabouts to identify the potential attacker. These counter-intelligence operations are useful for the company, and they have no interest in risking exposure with public criminal prosecution.

*[Third excerpt from chapter two –Proactive Tactics (partially) p. 133-171]*

**\*\* Please note that the selected excerpt covers only 3 tactics (out of 6). It should suffice to enable a discussion about Proactive Policing.**

## **The New Policing Strategy – Proactive Policing**

### **1) Proactive tactics**

There are several proactive policing tactics that all share some common principles: shifting the initiative from the criminal to the policing force; gaining access to operational intelligence prior to the commitment of a crime; getting control at effective intervention points for policing activity; and, crime-oriented policing that is tailored to the patterns of a particular crime.

We can identify a few predominant proactive tactics in cybercrime policing: 1) Operational and predictive intelligence; 2) Undercover entrapments; 3) Preventive architecture; 4) Operational surveillance; 5) Community policing; and, 6) Identity control.<sup>48</sup>

The use of various policing tactics enables law enforcement to adapt the appropriate tactic for each mission. Each tactic has its own pros and cons. Each is optimal for certain time spans, types of crime, or types of criminals. The tactics differ from each other in the relative degree of automation and the role for human discretion before taking action. They further differ from each other in the optimal points in the network for their deployment, and in the entity that is best suited to implement them. Many of the tactics – such as, undercover entrapment or predictive intelligence - can be implemented by both private and public entities. However, private and public entities may use them for different purposes and also in different form. There is a synergetic effect between the different tactics and the different operators of the tactics where they jointly create a multi-layered proactive system of policing. We will try to understand the relative advantages and disadvantages of each tactic and their operational mode.

---

<sup>48</sup> In a sense Identity Control is not an independent tactic, but an overarching method to facilitate optimal operation of all other tactics. We will further discuss it later.

Before I go further, a caveat: at this stage I am not advocating for any particular tactic or normatively encourage their use. As I will indicate later, I have many concerns about the use of certain tactics and the intensity of their use. Each tactic poses concerns about the depth of policing its intrusive nature, and its coercive effects. There are strong arguments why society may want to restrict a certain policing tactic or limit its use, even when the tactic proves very efficient. In other instances, predictive technology might be efficient in preventing crime, but would generally have a high rate of false positives. We may then want to use it for preventing certain crimes, but not for others.<sup>49</sup> At this stage, however, I aim only to describe the tactics. The discussion is mainly a description of the various technologies and policing operations that I have studied. However, certain technologies, that the tactics are based upon, are not yet fully developed, or the tactic has not sufficiently been tried to form a coherent mode of operation. In these cases, I will have to add an element of prediction to the description. Still, it is a prediction of a probable shape for certain tactics. These predictions are based on a technological and an operational reality and they are not normative suggestions. I do not believe in technological or social determinism, and certainly believe that it is in our hands to both shape the course of this technology, and to decide the nature of policing we want. For that, however, we first need to know what is possible, and what direction the technology and policing are likely to take.

---

<sup>49</sup> Kim Taipale in his writing indicates that we too often make general statements about the “efficiency” of a certain technology. However, in discussing the efficiency of a particular technology, we always need to ask whether it is efficient in connection to a particular task. A technology can be very efficient in predicting or preventing certain crime, yet very inefficient in relation to other crimes. Nevertheless, we too often make the mistake of “conclusions-transfer”; taking the conclusion that we reached in one context, and without question, transfer it to another context. This may prove to be very problematic. In the discussion about predictive preemption, for example, it is important to differentiate between its usage on crimes that follow a recognized pattern (e.g. credit card fraud), and malicious acts that do not follow a constant pattern (e.g. terror attacks). We must check the efficiency, false negatives and false positives, within the context of the targeted crime.

## 1) Operational and predictive intelligence

The new policing model is heavily dependent upon operational intelligence that can be acted upon prior to the crime to prevent it. This collected intelligence is normally different from the traditional intelligence that was collected in connection with a specific crime and often a particular suspect. This intelligence is composed of voluminous data about routine activities, which are often collected without any particular crime or suspect in mind. It is data about transactions, demographics, observed behavior, web usage, and communication traffic. Originally, this data is often not collected for policing purposes, but can serve for crime-oriented analysis. The collected data is “cleaned”<sup>50</sup>, and then analyzed to visualize and summarize normal behavioral patterns and suspected criminal behaviors. With new tools the data can be analyzed either from a central database or from distributed databases, which are managed separately.<sup>51</sup>

The collected data can further serve to build predictive models about criminal and anomalous behavior, or profiles of potential perpetrators. These models can be constructed from former hypothesis about the patterns of criminal behavior and attributes of criminals. Alternatively, in certain cases, the computer can find predictive patterns from the data without the need for former hypothesis. This process of pattern finding is also called *Data Mining*. The predictive patterns can then be employed for certain modes of preemptive policing operations: alerting investigators of suspicious activity, profiling individuals for different treatment based on risk potential, or real-time blocking or modification of traffic or transactions.

---

<sup>50</sup> On the process of “cleaning” data as the first phase in transforming data to be useful for analysis, see: Mary DeRosa, *Data Mining and Data Analysis for Counterterrorism*, CSIS, March 2004, 10. To be able to use the data later we need *data cleaning* that “can involve the removal of duplicate records, normalizing the values used to represent information in the database (e.g. ensuring that ‘no’ is represented as a 0 throughout the database, and not sometimes as a 0, sometimes as a N, etc.), accounting for missing data points, removing unneeded data fields, identifying anomalous data points (e.g. an individual whose age is shown as 142 years), and standardizing data formats (e.g., changing dates so they all include MM/DD/YYYY).” Jeffery W. Seifert, *Data Mining: An Overview*, CRS Report for Congress (December 16, 2004), 11.

<sup>51</sup> D. Jensen, *Data Mining in Networks*, Invited talk to the Roundtable on Social and Behavior Sciences and Terrorism, National Research Council, Division of Behavioral and Social Sciences and Education, Committee on Law and Justice. Washington, DC. December 11, 2002 (slides at: <http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02.html>).

Automated data analysis tools have become a central component of policing operations. They are necessary to overcome the human incapability to manually analyze large databases that are currently available for policing operations.<sup>52</sup> They are intended “to turn low-level data, usually too voluminous to understand, into higher forms (information or knowledge) that might be more compact (for example, a summary), more abstract (for example, a descriptive model), or more useful (for example, a predictive model).”<sup>53</sup> These tools currently serve both the public police and private entities to analyze and predict crimes, such as credit cards fraud, identity theft, auctions frauds, securities manipulations<sup>54</sup>, money laundering<sup>55</sup>, insurance fraud<sup>56</sup>, computer attacks (e.g. hacking, viruses, unauthorized access), internet scams, spam, copyright piracy, and child pornography.

---

<sup>52</sup> “The practical reasons driving development are the same in both the private and public sector – ‘vast data volume, fewer analytical resources’. The practical need for developing data-mining technologies is a direct result of the growth in data volumes. Traditional databases analysis relies on specific queries formulated by individual database analyst familiar with the particular data and database structure. This manual analysis is slow, expensive and highly subjective, and no longer able to manage the size and dimensionality of current data collection methods (Databases are increasing in two ways: (1) size, that is, the number of records or objects in the database and (2) dimensionality, that is, the number of fields or attributes to an object). As databases grow manual data analysis becomes impractical. Thus, the need to scale up human analytic capabilities through computational automation is driven by a practical (and unrelenting) imperative”, Kim A, Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 *Columbia Science & Technology Law Review* (2003) (Hereinafter: “Taipale, Data Mining”).

<sup>53</sup> Taipale, *Data Mining*, *Ibid*.

<sup>54</sup> Innovative Use of Artificial Intelligence - Monitoring NASDAQ for Potential Insider Trading and Fraud, AAAI News (<http://www.aaai.org/Pressroom/Releases/release-03-0917.html>) (“Better tools [developed] to monitor the market for suspicious activity that warrants closer inspection. The clues contained in the millions of trades, wire stories, and SEC filings each day makes it impossible for humans alone to sift through all the data to perform surveillance. To mine these vast stores of data, NASD has harnessed computers to sweep through all the data, identify and link items of potential interest, then present them to human analysts for further review. To mine the data, NASD has developed an intelligent surveillance application -- the Securities Observation, News Analysis and Regulation (SONAR) system -- that automatically monitors the NASDAQ, OTC, and futures markets for suspicious patterns. SONAR has been in operational use since December 2001. Each day it processes between 8,500 and 18,000 news wires stories, approximately 1,000 quarterly and annual SEC filings from corporations, and evaluates price-volume models for 25,000 securities. The system generates 50-to-60 alerts (“breaks”) per day for review by several groups of regulatory analysts and investigators...SONAR includes several AI techniques, such as data mining, natural language processing for text mining, intelligent software agents, rule-based inference, and knowledge-based data representation.”) See also: J. Dale Kirkland et al, *The NASD Regulation Advanced- Detection System (ADS)*, *AI Magazine* Vol. 20(1), Spring 1999, 55-67

<sup>55</sup> Ted E. Senator et al, [The Financial Crimes Enforcement Network AI System \(FAIS\)](#) Identifying Potential Money Laundering from Reports of Large Cash Transactions (1995) *AI Magazine* Vol. 16(4) 21-39; U.S. Congress, Office of Technology Assessment, *Information Technologies for the Control of Money Laundering*, OTA-ITC-630 (1995).

<sup>56</sup> George Cahlink, *Data Mining Taps the Trend*, *Government Executive Magazine*, October 1<sup>st</sup>, 2000

There is a heated public debate whether automated analysis tools and data mining technologies should be deployed to serve in the effort to locate potential terrorists<sup>57</sup> (due to their effect on privacy and their possible infringement of other civil liberties).<sup>58</sup> The public debate has led to certain legal restrictions and temporarily defunding the development of several data mining project, including the Total Information Awareness (TIA) project.<sup>59</sup> However, this legislative intervention is limited to a particular project, and does not cover classified projects or data mining projects run by the FBI and other law enforcement agencies.<sup>60</sup> It is therefore not surprising that, in domestic policing, these technologies are already heavily used both for street crime<sup>61</sup> and online crime.<sup>62</sup>

---

<sup>57</sup> The government is currently engaged in many classified development and testing projects that utilize automated data analysis tools and data mining technologies in fighting terror (see: Taipale, *Ibid*, \_\_\_). The main project, which received wide media attention, public debate and even a legislative response to defund it, is the Total Information Awareness (TIA) project. The project was part of a broader research plan at the Defense Advanced Research Projects Agency that was described as: "...language translation, data search with pattern recognition and privacy protection, and advanced collaborative and decision support tools. Language translation would enable the rapid analysis of foreign languages, both spoken and written, and allow analysis to quickly search the translated materials for clues about emerging threat. The data search, pattern recognition, and privacy protection technologies would permit analysts to search vast quantities of data for patterns that suggest terrorist activity while at the same time controlling access to the data, enforcing laws and policies, and ensuring detection of misuse of the information obtained. The collaborative reasoning and decision support technologies would allow analysts from different agencies to share data.", Department of Defense, Office of the Inspector General, Information Technology Management: Terrorism Information Awareness Project, December 2003, 7.

Another project that received wide attention is the Computer-Assisted Passenger Prescreening System (CAPPS II). This is a "rule-based system that uses the information provided by the passenger when purchasing the ticket to determine if the passenger fits into one of two categories: 'selects' requiring additional security screening and those who do not. CAPPS also compares the passenger name to those on a list of known or suspected terrorists. CAPPS II would have sent information provided by the passenger in the passenger name record (PNR), including full name, address, phone number, and date of birth, to commercial data providers for comparison to authenticate the identity of the passenger. The commercial data provider would have then transmitted a numerical score back to TSA indicating a particular risk level. Passengers with a 'green' score would have undergone 'normal screening', while passengers with a 'yellow' score would have undergone additional screening. Passengers with a 'red' score would not been allowed to board the flight, and would have received 'the attention of law enforcement.'", Jeffery W. Seifert, *Data Mining: An Overview*, CRS Report for Congress (December 16, 2004), 8-9.

<sup>58</sup> See: D. Jensen, *Data Mining in Networks*, Invited talk to the Roundtable on Social and Behavior Sciences and Terrorism. National Research Council, Division of Behavioral and Social Sciences and Education, Committee on Law and Justice. Washington, DC. December 11, 2002 (slides at: <http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02.html>); Technology and Privacy Advisory Committee Report, *Safeguarding Privacy in the Fight Against Terrorism* (March 2004); DeRosa, *Data Mining and Data Analysis*, *Ibid*; Taipale, *Data Mining*, *Ibid*;

<sup>59</sup> Jeffery W. Seifert, *Data Mining: An Overview*, CRS Report for Congress (December 16, 2004).

<sup>60</sup> Several legislative proposals are currently pending before Congress and the Senate to expand the regulation of data mining projects beyond the specific projects that were restricted or defunded. At the moment, however, there is no formal general limitation or other regulations regarding the development of

Based on predictive patterns, the new tools of database analysis serve in policing operations both against a pre-identified subject or groups of subject, and to identify not-yet-known potential criminals. **Subject-based queries**, “start with a specific and known subject and search for more information. The subject could be an identity – a suspect, an airline passenger, or a name on a watch list, for example, - or it could be something else specific, like a place or a telephone number. A subject-based query will seek more information about and more complete understanding of the subject, such as activities a person has engaged in or links to other people, places and things. It will also lead to other subjects that can be investigated”.<sup>63</sup> On the other hand, **Pattern-based queries**, “involve identifying some predictive model or pattern of behavior and searching for that in the data sets. These predictive models can be discovered through data mining, or they can come from outside knowledge – intelligence or expertise about the subject. However the patterns are obtained, the process involves looking for occurrences of these patterns of activity in data”.<sup>64</sup>

Subject-based policing follows the principle of traditional investigatory policing. It starts an investigation based on a particularized suspicion, and seeks out additional information. In contrast, pattern-based policing is a new concept that diverts from the traditional principle of particular suspicion and identified subject. “Pattern-based queries are less

---

data mining projects. Privacy advocates support general legislation to regulate the use of such technologies. See: Statement of James X. Dempsey, Executive Director of the Center for Democracy and Technology, The Defense of Privacy in the Hands of the Government, before the House Committee on the Judiciary, Subcommittee on Commercial and Administrative Law and Subcommittee on the Constitution, July 22, 2003.

<sup>61</sup> R.V. Hauck ET AL, Using Coplink to Analyze Criminal-Justice Data, IEEE Computer Vol. 35(3) 30-37 (2002).

<sup>62</sup> See for example the Matrix system which is “[A] program that ties together government and commercial databases in order to allow the authorities to conduct detailed searches on particular individuals, and to search for patterns in this data that can identify individuals possibly involved in terrorist or other criminal activities” (ACLU Issue Brief, The MATRIX: Total Information Awareness Reloaded – Data Mining Moves Into the States, at: <http://www.aclu.org/Files/OpenFile.cfm?id=15831>). On more crime-oriented programs using such tools see: General Accounting Office, Data Mining, Federal Efforts Cover a Wide Range of Uses, Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate, May 2004; Duncan Graham-Rowe, Cyber Detective Links up Crimes, NewScientist.com, December 5<sup>th</sup>, 2004; Andrew Johnson, Robot Cameras ‘Will Predict Crimes Before they Happen’, The Independent April 21<sup>st</sup>, 2002.

<sup>63</sup> Mary DeRosa, Data Mining and Data Analysis for Counterterrorism, CSIS Report, March 2004, 3-4.

<sup>64</sup> DeRosa, Ibid, at 4.

familiar in law enforcement and intelligence worlds in that they do not arise from a particular interest in a person, place, or thing. Instead, they seek information about people, places and things based on patterns of activity, none of the components of which might on its own arouse suspicion or be in any way improper.”<sup>65</sup> The following discussion will first discuss the use of subject-based queries in policing operations, and then explore pattern-based queries that are now being used in the new policing environment.

### **Preemptive criminal investigations**

The public police have been long interested in criminal intelligence investigations aimed at suspected criminal enterprises (organized crime) or potential terror groups. An intelligence investigation is directed to “determine the size and composition of the group involved, its geographic dimensions, its past acts and intended criminal goals, and its capacity to harm.”<sup>66</sup> It is not an investigation that primarily aims at prosecution, but at determining the organizational and operational structure of the illegal activity. It is a broad investigation that involves “the interrelation of various sources and types of information.”<sup>67</sup> These criminal intelligence investigations were uncommon in the physical world. They consumed immense resources, were very labor-intensive and difficult to manage. The collection and assembly of such information was a complex and dangerous task that risked human agents or involved constant, expensive surveillance operations. Even when the information was collected, it was hard to analyze, and even harder to find hidden knowledge in it. Therefore, “connecting the dots” from traditional analog information was a complicated challenge which too often suffered from an “imagination block”; when the investigators, who were following a pre-assumed investigatory hypothesis, organized the information accordingly.

The shift to digital databases and the new intelligence “building blocks” of voluminous data that can be analyzed with automated analysis tools, has changed the landscape of criminal intelligence investigations. Information scarcity is now replaced with data

---

<sup>65</sup> DeRosa, *Ibid*, at 5.

<sup>66</sup> The Attorney General Guidelines on Investigations.

<sup>67</sup> *United States v. United States District Court* 407 U.S. 297, 322 (1972).

abundance. Data is routinely collected and available for automated analysis. The focus is now on the collection and then the analysis of this “low-level” data instead of collecting high level intelligence. New services offer to aggregate commercial and public data sources and “clean” the data for optimized automated analysis, both private and public.<sup>68</sup>

Further, new tools enable to conduct *link-analysis*, which can map and visualize an association between various entities (e.g. individuals, organizations, places) and events (e.g. communication, meeting, purchasing). Each entity or event that is included in the dataset can then be subject to link-analysis to associate it with other entities and events. Link analysis “reveals the structure and content of a body of information by representing it as a set of interconnected, linked objects or entities. Often link analysis allows an investigator to identify association patterns, new emerging groups, and connection between suspects. Through the visualization of these entities and links, an investigator can gain an understanding of the strength of relationships and the frequency of contacts and discover new hidden associations... . Linkage data is typically modeled as a graph with nodes representing suspects of interest to the analyst and the links representing relationships or transactions.”<sup>69</sup>

Link-analysis tools are able to challenge the human “imagination block”. The discovered links are visualized, and then the investigator can change the subject at the center of the link-analysis with a click of a mouse. He is able to see the connection from the perspective of the suspected individual, the observed organization, a particular transaction, or specific communication, and find associations of interest. Moreover, link analysis can map the intensity, strength, direction, frequency and sequence of associations and events.

---

<sup>68</sup> Data aggregators collect data from various sources, including public records and private databases and conduct a process through which that data is “gathered, standardized, cleansed, matched, and expressed in a summary form, and periodically monitored and updated” (James Zimbardi, Data Aggregation vs. Data Mining, Presentation at the CSIS Data Mining Roundtable, July 2003).

<sup>69</sup> Jesu’s Mena, *Investigative Data Mining for Security and Criminal Detection* (2003), 76 (Hereinafter: “Mena”)

Link analysis can serve in various preemptive operations. It can visualize an ongoing activity, which can be indicative of a planned criminal behavior, that the investigator can then prevent with physical arrests, blockage of access, protection of potential target, or other preventive measures. Even though low-level data has limited evidentiary value for later prosecution, with the proper analysis, it can provide operational intelligence for effective preventive policing. Link analysis can also serve the investigator in evaluating the efficiency of possible alternative interventions. Link analysis tools are often able to interactively simulate “what-if” scenarios that aid in analyzing the probable effect of policing intervention in the criminal network. The investigator can, for example, simulate the dismantling of a specific individual (e.g. leader) or specific resource in the network (e.g. bank account) and find out what the effect will be on the criminal operational structure.<sup>70</sup> It enables the investigator to prioritize resources, and tailor the intervention to the particular criminal network.

### **Patterns based policing**

Automated tools also enable investigators to find patterns of criminal activities or attributes of criminal behavior to be able later to use them in a predictive manner. Developments in Artificial Intelligence technologies use computational modeling to find patterns of criminal behavior to differentiate it from legal behavior. Software systems that are modeled on the human process of learning and remembering<sup>71</sup> serve to tackle crime. “They mimic the cognitive neurological functions of the human brain. As such they are capable of predicting new observations from historical samples after executing a process of learning. A neural network can be used to detect a fraudulent transaction, a computer intrusion, and an assortment of other criminal activities, so long as examples of observations are available for training them.”<sup>72</sup>

---

<sup>70</sup> See about the use of such technologies to identify central members in a group: Hsinchun Chen et al, *Crime Data Mining: An Overview and Case Studies*, \_\_\_. See in also general about the use of social modeling in proactive forensic: James Okane, KPMG, *Exposing Fraudulent Transactions with Social Network Analysis*, Presentation at HTCIA conference 2004 (on file with author).

<sup>71</sup> Laurene Fausett, *Fundamentals of Neural Networks: Architecture, Algorithms and Applications* (1994).

<sup>72</sup> Mena, *Ibid*, at 159. It is important to note, however, that not all crimes are equally predictable and preventable using pattern recognition and pattern matching tools. Moreover, the efficiency considerations and social considerations in using these technologies may vary for different crimes. Scholars have focused on certain factors that affect the relative applicability of these tools: The volumes of historical data, the distribution between “proper” and “improper” behavior, the ability of criminals to adapt to new patterns of

Jesu's Mena explains the practical uses of these technologies in policing: *classification* – discriminating between two things based on similarities (e.g. distinguishing legal from fraudulent transaction); *clustering* – organizing observations into groups with similar features or attributes (e.g. group together criminals who perpetrate the same type of crimes); *Generalizing* – using examples to generalize about new cases or problems (e.g. modeling a “criminal signature”); *Forecasting* – looking at current information and predicting what is likely to happen. Prediction is a form of “classification into the future” (e.g. predicting fraudulent transaction).<sup>73</sup>

Once a pattern is recognized it can help to predict future crimes or find potential criminals in other datasets. The policing operation can systematically try to find these patterns in new datasets which are collected, and run them against historically collected data. Running recognized patterns against new datasets diverts from the normal principle of policing that search is based on a particular suspicion.<sup>74</sup>

Once a pattern-match is found there are varieties of policing options, both human and automated. Policing intervention can involve increased monitoring, blocking or modifying data traffic, denial of access, the opening of a criminal investigation, alerting a human operator for further decisions, and many other options. The decision whether to take a human action or automated action depends on the time intervals and the immediacy of required intervention.

---

behavior, the relative costs of false positive and false negatives, the changing patterns of legitimate behavior, the ability to adapt undesirable behavior to detection techniques, and the trade-off between accuracy for timely decisions and social consideration (such as privacy and discrimination). See: Tom Fawcett et al, AI Approaches to Fraud Detection and Risk Management, AAAI Magazine Summer 1998, Vol. 19(2), 107-108.

<sup>73</sup> Mena, Ibid, Chapter 6, Neural Networks: Classifying Patterns.

<sup>74</sup> See CDT's objection to data mining on the basis of the “Particularized Suspicion” principle, Statement of James X. Dempsey, Executive Director, Center for Democracy and Technology, America after 9/11: Freedom Preserved or Freedom Lost?, before the Senate Committee on the Judiciary November 18, 2003 (“The criminal standard and the principle of particularized suspicion keep the government from being diverted into investigations guided by politics, religion and ethnicity”).

To a large extent, patterns serve in *automated real-time policing*. A computer system is capable to recognize a pre-identified pattern in data or communication “on the fly” and then take immediate action. Once a pattern is recognized it is coded as a “crime signature”, and serves to block or modify traffic that matches the pattern. Intrusion detection systems, for example, that protects systems from hacking, viruses, denial of service and other forms of attack, use “signatures” as a main defense tactic. Spam filters and content filters also use “signatures” to block or modify flow of data. Since the intrusion detection systems or filters are positioned before the intended victim/ recipient they can shield him from the traffic that matches the “signature”.

Pattern recognition can operate either by identifying the “signature” of criminal or undesired behavior, or by identifying a deviation from normal expected behavior. Recognition of anomalous behavior (rather than criminal behavior) serves to compensate for the relative limited capability of “signature based protection.” “Signatures” codes, which are, again, a pre-identified indicator of undesired behavior, can only serve as a limited defense against new criminal modes of operation or a mutated pattern that diverts from the originally coded pattern. Therefore, this system often will also have protection against behavior that diverts (beyond a pre-defined level) from normal expected behavior.

75

In other words: while a “signature” identifies a recognized criminal behavior to defend from it, anomaly detection is coded with “normal behavior” and sets the alarm (or take action) when certain levels of deviation are discovered. Normal behavior correlates to the expected behavior of a user identification process, communication protocol structures, application behaviors, file format or many other details. Take, for example, a user who is

---

<sup>75</sup> See the model for designing Intrusion Detection systems: Dorothy E. Denning, An Intrusion Detection Model, IEEE Transactions on Software Engineering, SE-13, 222-232 (1987); Jake Ryan, Meng-Jang Lin and Risto Miikkulainen, Intrusion Detection with Neural Networks, Paper presented at the AAAI 1997 Workshop on AI Approaches to Fraud Detection and Risk Management (<http://nn.cs.utexas.edu/downloads/papers/ryan.intrusion.pdf>) (“Intrusion detection schemes can be classified into two categories: misuse and anomaly intrusion detection. Misuse refers to known attacks that exploit the known vulnerabilities of the system. Anomaly means unusual activity in general that could indicate an intrusion. If the observed activity of a user deviates from the expected behavior, an anomaly is said to occur.”).

normally at work between 9 a.m. and 5 p.m., logs in with his unique user name, and only uses word processor software, his internet browser, and regularly accesses the marketing division folder. This normal behavior can be coded as user-specific expected behavior. Then assume that one day the detection system finds that his user name logs-in at 1a.m., accesses the management division folder and tries to open an excel sheet document. The system can be programmed to identify this as an anomaly and take action, such as preventing access, requesting further telephonic identification process<sup>76</sup> or alert the security guards in the building.<sup>77</sup>

The use of policing through anomalies detection becomes an important tool; especially in an environment such as the internet where the identity of the victim is often random. As we discussed in Chapter One, online criminals often go after victims of opportunity, rather than victims of choice. Since the perpetrator has no prior information (or limited information) about the victim's normal behavior, the criminal is likely to conduct activities that deviate from the victim's normal activities. This is the place for detection system to alert of possible misuse; such as fraud or unauthorized access to an account. Take, for example, a criminal who steals credit cards and tries to use them in commercial transactions. If the transactions differ in dollar amount, type of products, location, and frequency from the normal credit card use, the system will alert of an anomaly.<sup>78</sup> In

---

<sup>76</sup> See in the context of systems against wireless phones' fraud and theft: "SearchSpace's technology monitors individuals' mobile phone use through intelligent plug-in software modules called sentinels, which create behavior profiles of network subscribers. Those behavioral profiles include the type of calls made, the numbers called, the length of calls and when they are made. According to SearchSpace, if suspicious activity on the account is detected, an alert is sent to the service provider, which in turn will employ an established response system to notify the phone user. The user might be required to enter a personal identification number (PIN) to verify his account, and the service might be terminated if the carrier not receive the correct response.", Jay Wrolstad, Erickson Enlists AI to fight Wireless Fraud, Wireless Newsfactor.com, February 5<sup>th</sup>, 2001.

<sup>77</sup> See also in the Credit Card usage context: "Neural networking techniques begin by analyzing a database, and using systematic methods to identify characteristic features, trends and patterns within the data. Such features can then be used to analyze fresh data and to predict whether or not it 'fits' the model. In cases of credit card fraud, for example, Gutschow said a stolen credit card often is used to make a self-service purchase at a gas station (to determine if the card is still active) immediately before it's used to buy jewelry or for some other major purchase. Such illicit transaction patterns really stand out when the system has been 'trained' to recognize the legitimate cardholder's usage pattern. An irregular transaction prompts an alert, which is transmitted instantly to the sales clerk handling the purchase.", Bruce V. Bigelow, Computers Try to Outthink Terrorists, The San Diego Union-Tribune, January 13, 2002.

<sup>78</sup> Mena discusses the common detection technique for credit card fraud: "Look for lead indicators. Loss will inevitably occur before detection. Sequencing of purchases will change; the merchant mix will be out

practice we see more and more security systems that focus on anomaly detection as the major tool for crime prevention. It takes some time to “train” the system to recognize normal, expected behavior (of a user, network or software application), but it creates a powerful policing tool. As the system gets more and more sophisticated in identifying normal behavior through various measured variables, it produces less false positives and less false negatives.<sup>79</sup>

Real-time policing of data traffic, which is based on patterns (either “signatures” or anomaly detection), tends to favor automated intervention over human intervention. On the other hand, predictive policing, which runs patterns against databases to find potential future crimes and potential criminals, often involves a hybrid of automated pattern-matching searches and human analysis and intervention.

### **Profiles based policing**

A supplementary tool, often used in tandem with pattern matching, is automated profiling. A computer system can learn to develop profiles of criminals or predictive profiles of criminal activities. The profiles are constructed with the use of machine-learning algorithms. “These software programs can be used to develop profiles of perpetrators through a combination of decision trees and conditional IF/THEN rules... using machine-learning and statistical algorithms... conditional constructs of criminal attributes and features can be extracted from large databases.” The output of these tools “is highly descriptive in their classification of a desired solution, such as the conditions leading to criminal act like fraud, or the attributes and features of criminals.”<sup>80</sup>

---

of character compared to previous consumer transactions. Frequency, monetary, and recency (FMR) techniques can be examined and employed. Time-sequence accumulated-risk scores may be used as an input to aggregated risk exposure. A change in location may indicate a ring operation. There are a number of leads that relate specifically to credit-card and debit-card fraud. They are common points-of-purchase (CPP) detection, particularly with regard to new merchant agents. The main method of detection is to look for outliers and changes in the normal pattern of usage. A SOM neural network can be used to perform an autonomous clustering of patterns in the data.”, Mena, Ibid, 277.

<sup>79</sup> See for example: Jake Ryan, Meng-Jang Lin and Risto Miikkulainen, Intrusion Detection with Neural Networks, Paper presented at the AAI 1997 Workshop on AI Approaches to Fraud Detection and Risk Management (<http://nn.cs.utexas.edu/downloads/papers/ryan.intrusion.pdf>).

<sup>80</sup> Mena, Ibid, 205.

Jesu's Mena demonstrates, for example, how with a machine-learning algorithm an analyst can generate a set of rules for profiling a potential smuggler at a point-of-entry border crossing:

“If Vehicle Make is Chevrolet,  
AND Year of Vehicle is 1998,  
AND No Insurance Listed for the Vehicle  
AND Lien Holder is Owned,  
THEN there is  
06.34% chance that Alert is Low  
18.32% chance that Alert is Medium  
75.33% chance that Alert is High

The Rules are generated from an analysis of thousands of observations leading to a list of conditions (IF/AND) and a prediction (THEN) with a probability value associated with it (75.33%). The rules from these types of data mining analysis be viewed as a ratio of conditions, which when combined, lead to predicted outcome with an associated probability.”<sup>81</sup>

These tools help analysts to predict, from databases, the probability of crime and to profile criminals into statistically significant clusters or segments. These tools - like the neural networks that we discussed before – “need to operate on samples of legal versus illegal transactions or criminals versus legitimate individuals. However, unlike neural networks, the output, in the form of either rules or graphical decision trees, is easy for humans to comprehend.”<sup>82</sup> The machine learning algorithm works by posing a series of questions against the database. This is done to understand which variables are statistically most significant in determining a profile of a criminal, or the conditions of a criminal act.<sup>83</sup>

---

<sup>81</sup> Mena, Ibid, 205-206.

<sup>82</sup> Mena, Ibid, 206.

<sup>83</sup> The use of machine-learning tools enables investigators to find the most significant variable (or variables) to predict a certain outcome. In a database that may include handful of different variables, it helps to find which of these we should focus on. These tools are very important outside the criminal policing context. For example, Malcolm Gladwell in his recent book “Blink – The Power of Thinking Without Thinking” discusses the use of such tools to find the most important variable in predicting whether a patient that comes to the emergency room may be suffering from a heart attack. This prediction can then

These tools have become of primary importance online. They serve to predict auction fraud, spam, credit card fraud<sup>84</sup>, securities manipulation and many other crimes. Often the profiling tools will be used in combination with pattern recognition tools to enjoy the relative advantages of both.<sup>85</sup> The commercial tools of fraud detection, for example, normally use modular architecture that combines some or all of the different automated analysis tools that we have discussed. These tools are multi-layered and include detection of patterns of misuse, anomaly detection, and profiling.<sup>86</sup>

At the end, each of the crime predictors (pattern-matching, anomaly detection and profiling) results in a continuous value number. This number states the probability of a particular activity to be a crime or a particular user to be a criminal. The detection and prevention tools combine the results of the different predictors to come up with a single **Risk Score**. For example, in a system that detects fraud, the risk score will represent the likelihood that the transaction is fraudulent. Currently online systems assign risk scores for every individual credit-card transaction or online auction. The same is true with filters that assign risk scores for each e-mail to predict whether it is spam.<sup>87</sup>

---

serve the hospital in prioritizing patients for hospitalization, when there is a scarcity in beds. Apparently, doctors, who are asked to perform the same task without automated tools, would normally focus on variables that are of limited statistical significance. In comparison, the variables generated by automated tools are statistically more significant., See: Malcolm Gladwell, *Blink – The Power of Thinking Without Thinking* (2005).

<sup>84</sup> Visa EU Launches New Advanced Fraud Detection Tool, Visa Press Release December 29<sup>th</sup>, 2003 ([http://www.visaeu.com/pressandmedia/press178\\_pressreleases.html](http://www.visaeu.com/pressandmedia/press178_pressreleases.html)) (“the use of rules allows you to create cases for a particular merchant, merchant type or country that is specifically affecting you as an issuer – regardless of whether this is a problem other issuers are experiencing.”)

<sup>85</sup> Tom Fawcett and Foster Provost, *Combining Data Mining and Machine Learning for Effective Fraud Detection*, Paper presented at AAAI 1997 Workshop on AI Approaches to Fraud Detection and Risk Management.

<sup>86</sup> See for example the architecture of Falcon Fraud Manager Product that serves for real-time detection of fraud in various industries ([http://www.fairisaac.com/NR/rdonlyres/416B141F-E807-48AE-AA2E-51562B7E729E/0/FalconFraudManager\\_PS.pdf](http://www.fairisaac.com/NR/rdonlyres/416B141F-E807-48AE-AA2E-51562B7E729E/0/FalconFraudManager_PS.pdf)). The product combines various modules including: Profiling technology (“Identifies key transaction behaviors and spending patterns for each account to ensure easy recognition of uncharacteristic expenditures”), Neural network modeling (“Predictive models available based on transaction data and cardholder profiles”), Consortium or Custom models (“Incorporate data from hundreds of card issuers, Custom models represent unique data”), Transaction-based scoring (“Analyzes each authorization transaction to assess risk of fraudulent activity. Provides an accurate transaction fraud score, indicating the likelihood of the transaction to be fraudulent”), and Analyst Workstation.

<sup>87</sup> Heinz Tschabitscher, *What Do You Need to Know about Bayesian Spam Filtering*, About.com ([http://email.about.com/cs/bayesianfilters/a/bayesian\\_filter.htm](http://email.about.com/cs/bayesianfilters/a/bayesian_filter.htm)); Flavio D. Garcia, Jaap-Henk Hopeman &

The detection and prevention systems follow rules that dictate what the consequence of a particular risk score will be. “The risk score is compared against a predetermined score threshold, thereby enabling acceptance or firing of an alert”.<sup>88</sup> The system can be designed for different levels of sensitivity for the score threshold that will result in a preventive action. Further, the system can have a menu of preventive measures which has broader implications than just enabling or denying activity (e.g. authorizing transaction or routing e-mail).<sup>89</sup> A fraud detection system can, for example, be set to authorize a transaction that results in a risk score lower than 90; require further identification for a transaction that results in a risk score between 90 and 95; and deny authorization for transaction that has a risk score higher than 95.<sup>90</sup>

The method of comparing a Risk Score against a predetermined Score Threshold is common in detection and prevention systems for various different crimes. A score threshold is set for blocking e-mail that is suspected of being a spam or containing malicious codes, authorizing credit card transactions, monitoring online auctions, and filtering content. The same method is also being currently tried for systems that aim to identify potential terrorists at the airport, and to decide what security procedures a

---

Jeroen Van Nieuwenhuizen, Spam Filter Analysis ([http://arxiv.org/PS\\_cache/cs/pdf/0402/0402046.pdf](http://arxiv.org/PS_cache/cs/pdf/0402/0402046.pdf)). See for example the product description of a common Spam filter by Astaro: “Astaro’s Spam Protection (Spam Filter) scans inbound e-mail messages (SMTP and POP3 protocols). It performs a series of tests and assigns a ‘Spam Score’ to each message indicating the probability that the message is unsolicited. Message whose score exceeds thresholds, set by the administrator, are dropped, returned to the sender, passed to the recipient with a warning or quarantined. Astro’s Spam filter utilizes multiple methods to pierce the disguises used by professional spammers: **Sender Address verification**... **Realtime Blackhole Lists (RBLs)**... **Header Analysis** – The Header section of emails are checked for false or alerted information and addresses with invalid characters... **Body Analysis (Heuristics)** – Words and word patterns of spam are identified... **Whitelist and Blacklist** – the administrator can list email sources known to be legitimate and illegitimate. The result of all tests are incorporated in the ‘Spam Score’ that indicated the probability that the message is unsolicited.” ([http://www.astaro.com/firewall\\_network\\_security/anti\\_spam\\_filter](http://www.astaro.com/firewall_network_security/anti_spam_filter)).

<sup>88</sup> Mena, Ibid, 252.

<sup>89</sup> See also the process of Risk Scoring and the security results of different scores within the context of screening passengers for preflight security with the use of CAPPS II system (which has been canceled and replaced by another project): Jeffery W. Seifert, Data Mining: An Overview, CRS Report for Congress (December 16, 2004), 8-9.

<sup>90</sup> The rule about the result of a particular risk score will often also be “personalized” for different customers. It can include an “historic memory”, which calculates the previous risk scores for each individual. If a particular individual had several risk scores that passed the general rule, but were just a little below the alert threshold, another high risk score could lead to an alert even if it is still below the general alert threshold.

passenger will undergo. The major dilemma in all these scenarios is what level to set the Score Threshold. Different thresholds imply different potential costs (both in monetary and privacy terms) regarding false positives and false negatives.

## 2) Undercover stings

Online policing uses undercover operations as a dominant tactic to proactively tackle crime. Undercover operations are common also in the offline policing<sup>91</sup>, but become cheaper, easier to operate, risk-free, and scalable, online. They often do not include the legal difficulties – mainly the entrapment defense - that restrain the police from using offline undercover operations on a large scale. A single person (policeman, private security of private vigilantes - Hereinafter “undercover operator”) can automatically and simultaneously run many complex undercover operations. He can also enjoy the anonymity of the internet to create multiple online personas for undercover operations. The investigatory guidelines traditionally limited the use of undercover operations, and required a long internal approval procedure for such operations. These were replaced by permissive guidelines that encourage the use of undercover tactics online and offline.<sup>92</sup> In addition, private security assigns undercover operations an important role in its multi-layered defense plan. Currently, undercover operations are used by both private and public entities to proactively tackle various online crimes such as hacking, spam, child pornography, pedophilia, trade secrets' theft, fraud, copyright piracy and many other crimes.

Undercover operations follow three different modes of operation: 1) Undercover operator posing as a *participant* in the unlawful activity (.e.g. the government operates a child pornography server) 2) Undercover operator posing as a *prospective victim* of the unlawful activity (.e.g. undercover agent impersonating a teenager in a chat room to lure pedophiles, or a honeypot system which lures unauthorized users); and 3) Undercover operations aiming to mark users or resources to enable *identification* at a later, potential criminal event (e.g. fingerprinting a document or software that may be used in crime).

---

<sup>91</sup> The Attorney's General Guidelines on Federal Bureau of Investigation Undercover Operations; Gary T. Marx, Undercover – Police Surveillance in America (1988). On the use of offline undercover operations by private entities see: Arthur Hulnick, Dirty Tricks for Profit: Covert Action in Private Industry, 14 International Journal of Intelligence and Counterintelligence 529 (2001).

<sup>92</sup> The Attorney's General Guidelines on Federal Bureau of Investigation Undercover Operations. The change in the guidelines affects the conduct of online undercover operations. Yet, it first of all meant to encourage the use of offline undercover operation as part of the overall trend to shift to preventive policing in the fight against terror and organized crime.

We will come back to elaborate on each of these modes of operation, after we first understand the rationale beyond undercover operations.

Traditionally, undercover operations were mainly used to “encourage” a criminal to attempt to conduct an unlawful activity, arrest him and then prosecute him for the attempt. This is, for example, the case with an undercover policeman who poses as a drug buyer to “encourage” a drug dealer to sell him drugs. When the dealer hands him the drugs, he is arrested and prosecuted for the attempt to commit the crime of drug dealing.<sup>93</sup> Online undercover operations sometimes use the same format (e.g. prosecuting a pedophile for attempting to molest someone who was identified as a minor online).<sup>94</sup> Yet, often online undercover operations are not aimed at prosecution. They attempt to gain information about potential patterns of crime, track trends in online crime, identify a propagating crime at early stage, or assess risk. They may also try to preempt crime (rather than prosecute) by disarming the perpetrator (e.g. disabling the attack tool), or deflecting the criminal activity to a protected zone (e.g. non productive systems).<sup>95</sup>

Undercover operations also aim to affect the behavior of potential criminals and deter their activity. These operations increase the cost of crime (if a criminal wastes resources on bogus targets); decrease the perceived gain; and increase the probability of penalty (since the criminal may be dealing with an undercover operator). All this produces higher levels of deterrence to criminal activity when a potential criminal knows that undercover operations take place. Furthermore, undercover operations affect behavior by creating distrust between potential participants in the criminal activity (such as in collaborators, or buyer-seller relationships).<sup>96</sup> The awareness of undercover operations creates, for

---

<sup>93</sup> For recent uses of undercover operation offline, see: Rachel Clarke, What is a Legal Sting?, BBC News, September 23<sup>rd</sup>, 2003.

<sup>94</sup> Carl Hessler, Online Sex Stings Snare Claims of Entrapment, The Mercury, 06/07/2004.

<sup>95</sup> The discussion about deflection of crime differentiates between deflection of crime from one victim to another which is socially unhelpful, and deflection of crime that decreases the amount of criminal activity or mitigates its effect. See footnote \_\_\_\_.

<sup>96</sup> Bruce Hay speaks of the different designs of sting operations that aim to gain information about potential criminals and those that aim at deterring potential criminals: “Sometimes it is quite clear that the government is trying to catch and punish wrongdoers. This is most evident in cases where .... The

example, distrust between a drug dealer and the potential buyers, since there is always the possibility they may be undercover agents. Due to the nature of online criminal collaborations, which we discussed in Chapter One, creating distrust among online criminals is an important mission of online policing. It aims, for example, to create distrust between malicious code writers and script kiddies; who then download the codes and execute them. Participants of the relevant sub-cultures, have repeatedly raised the concern about the government seizing the distribution nodes for attack tools and spread other tools; which seem to come from hackers. The script kiddies are afraid to use a code that might have been implanted by the government and can potentially track their activities or harm their machines. A similar tactic is used to create distrust between file-sharing traders of copyrighted work or sellers and buyers of child pornography.

Using an undercover operator as a participant in criminal activity is often criticized as an improper policing tactic that encourages criminal activity. However, the law recognizes it as a necessary evil to investigate certain type of crimes that otherwise would be hard to prevent or prosecute.<sup>97</sup> Yet, to protect the public from undue policing practices, the entrapment doctrine safeguards the defendant.<sup>98</sup> “Entrapment occurs when the government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of that offense in order to prosecute.”<sup>99</sup> This doctrine assures that *objectively* the police do not

---

existence of the operation is kept a well-guarded secret. The idea is to get the wrongdoer to trust the undercover agent so that he will commit his crime in ‘plain view’ (that is, in front of surveillance cameras). If catching the criminal is the objective, the more the target believes his apparent confederates or victims are genuine, the better. In deterrent sting, the opposite holds. The government wants to sow the distrust among crooks, so that (ideally) every crook is afraid of his confederates or victims are agents. This is why the government widely publicizes the existence of sting operations.” Bruce Lay, *Sting Operations, Undercover Agents, and Entrapment*, The Harvard John M. Olin Discussion Papers Series, Discussion Paper No. 441 (10/2003) (at: [http://www.law.harvard.edu/programs/olin\\_center/](http://www.law.harvard.edu/programs/olin_center/)).

<sup>97</sup> “The use of undercover techniques, including proprietary business entities, is essential to the detection, prevention, and prosecution of white collar crimes, public corruption, terrorism, organized crime, offenses involving controlled substances, and other priority areas of investigation.”, The Attorney’s General Guidelines on Federal Bureau of Investigation Undercover Operations).

<sup>98</sup> See: ; “In their Zeal to enforce the law, however, government agents may not originate a criminal design, implant in an innocent person’s mind the disposition to commit a criminal act, and then induce commission of the crime so that the government may prosecute”, *Jacobson v. U.S.* 503 U.S. 540, 548 (1992). On the history of the entrapment defense see: Rebecca Roiphe, *The Serpent Beguiled Me: a History of the Entrapment Defense*, 22 *Seaton Hall Law Review* 257 (2003).

<sup>99</sup> The Attorney’s General Guidelines on Federal Bureau of Investigation Undercover Operations.

use tactics that induce innocent people to criminal activities that they are not predisposed to; and that *subjectively* a defendant is convicted only if he was predisposed to commit the crime anyhow.<sup>100</sup> It is important to note, however, that the doctrine is limited and does not cover undercover operations that are carried out by private parties.

This doctrine informs the internal procedure for the police in using undercover operations, and directs them to set a restrictive policy for offline undercover operations. With the shift online, the entrapment doctrine does not seem to pose the same set of problems to undercover operations.<sup>101</sup> First, many of the undercover operations are put in motion by private entities, which are not covered by the doctrine. Second, the operation can be constructed so that the government is not actively searching for potential criminals, but passively waiting for those who are predisposed towards a certain crime (e.g. traders of child pornography).<sup>102</sup> The government can take control over a criminal website, such as child pornography trade site, and operate it in the same format as the criminal owner. The government, in these cases, creates no additional inducement to commit crime.

In practice, both the government and private entities often use undercover operations in which the agent is a participant in the crime. The public police operate websites that offer criminal content, such as child pornography, to track people who upload and trade content. In few operations, the police established a website, which claimed to host child pornography, then used the cooperation of search engines to rank the site high in search

---

<sup>53</sup> For more on the interplay between the “objective” element and the “subjective” element in the entrapment doctrine see: Dru Stevenson, Entrapment and the Problem of Deterring Police Misconduct, 37 Connecticut Law Review 67 (2004).

<sup>101</sup> Jennifer Gregg, Caught in the Web: Entrapment in Cyberspace, 19 Hastings Communications and Entertainment Law Journal 157 (1996); N. Brovet, Entrapment in Cyberspace: Are Traditional Entrapment Doctrines Sufficient to Protect Internet Users from Unreasonable Police Conduct?, Michigan Telecommunications and Technology Law Review Vol. 5 (1998).

<sup>102</sup> Aaron M. Bailey, A Nation of Felons?: Nepstar, the Net Act, and the Criminal Prosecution of File-Sharing, 50 American University Law Review 473, 530 (2000).

results, to attract people who sought child pornography.<sup>103</sup> These operations led to the successful prosecution of thousands of child pornography buyers. Alternatively, the police seized websites that had already been used for illegal activity, and tracked the activity to find the criminals.<sup>104</sup> Recently, in “Operation Web Sweep”, the New Jersey police coordinated an international operation to locate users of a child pornography server which they seized<sup>105</sup> and then operated.<sup>106</sup> The police can gain control of illegal websites by offering the operator who is arrested a great deal: let us operate the website to find other criminals, and you’ll go free or get reduced punishment, on the condition that you do not disclose that you no longer operate the site.<sup>107</sup>

---

<sup>103</sup> See for example the details of “Operation Pin” where “law enforcement agencies behind Operation Pin have worked with search engine operators to ensure that fake sites appear when someone looks for particular keywords” (Mark Ward, Online Dragnet to Thwart Pedophiles, BBC News, December 18, 2003).

<sup>104</sup> Declan McCullagh, Police Powers Move Into Your Browser, ZDNet News, March 3, 2003.

<sup>105</sup> In other cases, the police have seized websites that offered illegal content and used them to post a warning to potential users of that website. See for example the site <http://www.420now.com> that used to offer drug paraphernalia such as marijuana cigarette holders for sale. The police, after seizing the site, posted the following warning: “By application of the United States Drug Enforcement Administration, the website you are attempting to visit has been restrained by the United States District Court for the Western District of Pennsylvania pursuant to Title 21, United States Code, Section 853(e)(1)(A).”

<sup>106</sup> After the New Jersey investigators located and seized a website that offered child pornography for monthly subscription, they started “Operation Web Sweep”. “In February 2002, the Division of Criminal Justice Computer Analysis and Technology Unit disabled the site and removed all child pornography. ‘Operation Web Sweep’ was implemented and a ‘replacement’ website at the same domain address was created. The replacement website, which contained no illegal content, was visually styled in the same fashion of the original website. The site informed prior or prospective subscribers that the site had incurred technical difficulties and that it was in the process of rebuilding a collection of images. Through an assigned username and password, subscribers could upload or transmit pictures to the site. As ‘subscribers’ and others ‘visited’ the site, Criminal Justice investigators determined the international scope of the investigation and sought the assistance of the FBU, the U.S. Attorney’s office and the New Jersey National Center for Missing and Exploited Children. Additionally, law enforcement agencies from the various foreign nations were notified and participated in the investigation... To date, the investigation has identified nearly 200 potential suspects in 16 nations... execution of court authorized search and seizure warrants at the residences and/or business locations of those individuals who subscribe to the site and who provided child pornography images.”, New Jersey Division of Criminal Justice Coordinates International Investigation & Cyber-Sting Operation Tracking Distributors of Internet Child Pornography, Criminal Justice News, May 8, 2002.

<sup>107</sup> In other operations, however, the police created their own phony website to lure potential criminals. In some of these cases the government, in my opinion, crosses the line between a legitimate sting operation, and actual inducement for crime. The arrested people might have been fantasizing about committing this crime, but there is doubt whether there were predisposed to actually commit it. However, the courts seem to approve of online stings even in such cases. See, for example, the recent “Operation Turnaround” which the FBI used to fight sex tourism. In this operation, the FBI set a phony travel agency web site. “‘The idea was that we would mirror what was actually happening out there, so here we used the same techniques that are being used by underground travel agencies and other individuals and we copied their techniques’, FBI Agent Terri said” (FBI Busts 11 People in Child Sex Sting Operation, nbc6.net, April 4<sup>th</sup>, 2005 (<http://www.nbc6.net/news/4345336/details.html>)). “None of those arrested in the sting actually had sex with kids; they were busted for their intentions. Police said they arranged to have sex with children by

The government is also cooperating with private entities by embedding undercover operations in their websites. EBay, the online marketplace and auctions website, lets the government use “manufactured” identities to participate in suspicious auctions (e.g. sold items that are suspected as contraband or a fraudulent auction).<sup>108</sup> The police agent will participate in the auction, as either a buyer or a seller, to make a contact with the suspect or follow the transaction. EBay helps the government by establishing a credible identity for the governmental agent, with a “manufactured” history of sells and feedbacks which doesn’t raise suspicion. If, in physical undercover operations, it is difficult for the police agent to penetrate the criminal network and create a credible persona, such a persona can be “manufactured” online very easily.

Furthermore, the government can use the internet to create the image of a credible activity to lure pre-identified suspects. In the case of *Ivanov*<sup>109</sup>, the government was facing Russian hackers who were attacking online U.S. based companies, and extorting them with threats of further attacks. The FBI faced non-cooperating foreign investigators, and decided to lure the hackers to the U.S.. Using an internet presence with minimal costs, the FBI was able to create a credible image of business activity of a security company. The "company" then invited the hackers to come to the U.S. to negotiate employment options. The hackers who came to the U.S. met with the “company directors” (the FBI agents), and were arrested after demonstrating their hacking skills, thus providing evidence for prosecution. In this case, the virtual nature of the internet

---

booking sex tour packages on a Web site called ‘Costa Rica Taboo Vacations’. The site said the vacations were ‘for the discrete male’, and said it was ‘where all your personal desires are fulfilled’, with ‘companions supplied 24 hours a day’. The Web site had bogus testimonies from satisfied customers. Agents arrested most of the clients at Miami International Airport just before they boarded airplanes bound to Costa Rica.” David Marcus, the lawyer representing one of the arrested suspects, argued against this practice: “Their Web site got 25,000 hits per day... But there are no children, there was no sex, and these FBI agents are highly skilled at how to reel these people in, just for their thoughts, not for their actions.”

<sup>108</sup> See: Ernest Miller & Nimrod Kozlovski, eBay to Law Enforcement – We’re Here to Help, Lameme, February 17, 2003 (<http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=925>).

<sup>109</sup> U.S. V. Ivanov 175 F. Supp. 2d 367 (D. Conn., 2001); Nathan Thornburg, 2 Russian Hackers Nabbed in FBI Sting, Moscow Times, April 28<sup>th</sup>, 2001.

enabled the FBI to create a facade of legitimate business activity. Such an operation would have consumed immense resources if it were established offline.<sup>110</sup>

However, the major change in undercover operations relates to the use of undercover agents posing as victims. This mode of operation in offline policing is very risky, labor-intensive, and requires the full attention of the police during the time of its deployment (e.g. female agent who is used as bait for rapist). For these reasons and others, it has never been a common tactic. In contrast, it has become the online predominant mode of operation. Both private entities and the public police use it either in human-agent mode (e.g. agents engaging pedophiles on chat rooms) or in an automated fashion (e.g. Honeypot). It is cheap to operate, requires limited manpower (if any), and involves no risk.

This mode of operation serves as a major element in the fight against pedophiles.<sup>111</sup> An agent can enter a chat room to seek out potential pedophiles. He can impersonate a teenager and engage in a conversation with others in the chat room.<sup>112</sup> His aim is to lure the pedophile into making explicit statements about his unlawful desires towards a minor. After such statements are made, the agent will often try to lure the pedophile into arranging a physical meeting with the “minor”. At that meeting, the pedophile will be

---

<sup>110</sup> The police have also been using fake companies in offline undercover operations. These business entities are called “Proprietary” in the investigatory jargon (“‘Proprietary’ means a sole proprietorship, corporation or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationships with the FBI is concealed from third parties”, The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations). The problem with such business entities is that it requires expensive resources and manpower to create the facade of a legitimate business. Moreover, once the business is exposed by the criminals who are prosecuted, it can no longer efficiently serve for further undercover operations. In contrast, online it is easy to create many fake businesses with seemingly legitimate activity, and once a particular business is exposed, the police can shift to another virtual business.

<sup>111</sup> Jennifer Gregg, Caught in the Web: Entrapment in Cyberspace, 19 Hastings Communications and Entertainment Law Journal 157 (1996); Christa M. Book, Do You Really Know Who is on the Other Side of Your Computer Screen? Stopping Internet Crimes against Children, 14 Albany Law Journal of Science and Technology 749 (2004).

<sup>112</sup> Stalking Child Molesters on the Net, Tripod.com (at: [http://alterboys.tripod.com/Child\\_Abuse\\_Ne/Learn\\_Morex.html](http://alterboys.tripod.com/Child_Abuse_Ne/Learn_Morex.html)).

arrested for attempting to molest a child.<sup>113</sup> The police are currently encouraging this mode of operation; training agents to conduct these undercover conversations, and publicizing these operations to deter potential pedophiles. Private vigilantes are also often involved in such undercover operations. Some of these vigilantes inform the police when they identify a potential pedophile, other use the interaction with the pedophile to gain identifying information about him, and shame him publicly.<sup>114</sup>

New automated tools are being introduced to assist in chasing pedophiles. Automated agents (Bots) can search the web to identify potential presence of pedophiles in chat rooms (through content analysis of the conversation and other indicators). In addition, software can compare conversations from different chats to identify whether the messages are likely to have come from the same actor. This helps to correlate cases and to gain intelligence about the potential pedophile who the agent tries to engage in conversation. Furthermore, new tools enable agents to identify a potential lie in a conversation, and therefore indicate to the agent about the state of mind of his conversations' partner (e.g. whether he is indeed a teenager as he claims). These tools have no evidentiary value in court, but they serve to direct the agent towards the desired result.

Beside these undercover operations that are operated by human agents also dramatically increases the use of *automated decoys*, such as a Honeypot. Online security takes another step, using the idea from Winnie-the-Pooh, “a stuffed bear who was lured into various

---

<sup>113</sup> This practice is often criticized as active inducement and as “policing of the mind” since no crime was actually committed. Defendants have also often claimed that they knew all along that there wasn't a minor involved and it was only a “fantasy game” (more on the “fantasy defense see: Donald S. Yamagami, Prosecuting Cyber-Pedophiles: How can Intent be Shown in a Virtual World in light of the Fantasy Defense, 41 Santa Clara Law Review 547 (2001)). The courts are usually not sympathetic to these claims and rarely discharge an adult who engaged in conversations of frank sexual content and later arranged for a physical meeting with someone who was identified as minor. See: Jon Frank, Talking Dirty to a 44-Year-Old Man, Virginia-Pilot, January 15, 2003 (at: [www.mail-archive.com/cyberpunks@minder.net/msg33948.html](http://www.mail-archive.com/cyberpunks@minder.net/msg33948.html)). ;Carl Hessler, Online Sex Stings Snare Claims of Entrapment, The Mercuray, 06/07/2004.

<sup>114</sup> Vigilantes opened websites in which they post the content of the conversation with the alleged potential pedophile aside the identifying information they collected about him. See:

predicaments by his desire for pots of honey.”<sup>115</sup> In computer terminology, a Honeytrap is a trap which is set to detect or deflect attempts at unauthorized use of information systems. “Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information that would be of value to attackers.”<sup>116</sup> It is “resource whose value is [in] being attacked or compromised”.<sup>117</sup> In other words: a Honeytrap consists of a computer system or a network that has no value to the production system. It is set as intentional bait to lure attackers to the system, who believe that they are attacking a legitimate production system.<sup>118</sup> To look more attractive to potential attacker, it will often include files with tempting names for an intruder (such as “confidential reports”). With the recent developments in Honeytraps, software can simulate a fake network of thousands of computers which are really operating from a single computer. This facade can be configured with arbitrary services, and create the impression of an important network to an external attacker.<sup>119</sup> The Honeytrap constantly monitors the system and logs every activity, collecting evidence for later prosecution or information to be analyzed for security purposes.

---

<sup>115</sup> Wikipedia’s definition of “Honeytrap”.

<sup>116</sup> Wikipedia, Ibid, there. See also the definition given by Ian Walden and Anne Flanagan: “A Honeytrap or deception host is a designated area within a computer system or network that has been designed specifically with the expectation that it will be attacked by unauthorized users, whether internal or external to the organization operating the honeytrap.” Ian Walden & Anne Flanagan, Honeytraps: A Sticky Legal Landscape?, 29 Rutgers Computer & Technology Law Journal 317, 318 (2003).

<sup>117</sup> Lance Spitzner, The Value of Honeytraps, Part One: Definitions and Values of Honeytraps, SecurityFocus, October 10, 2001. See more: Kellep A. Charles, CISSP, Decoy Systems: A New Player in Network Security and Computer Incident Response, International Journal of Digital Evidence, Vol. 2 Issue 3 (Winter 2004).

<sup>118</sup> In order to deceive a potential attacker the Honeytrap needs to resemble a legitimate system. “To deceive, a honeytrap must provide realistic responses to requests so that an attacker does not suspect it is a trap. Details such as password files, service banners, and file permissions should be configured and dynamic activity should be realistic.” Brian Scottberg, William Yurcik and David Doss, Internet Honeytraps: Protection or Entrapment? IEEE International Symposium on Technology and Society, June 2002.

<sup>119</sup> In computer security technology there is a distinction between honeytraps based on the level of interaction. *Low-interaction honeytraps* are primarily software that emulate (imitate) different operating systems and services. It is cheaper and easier to operate such a honeytrap, but they capture only limited information. *High interaction honeytraps* do not emulate. They are real computers, applications and services which are provided in an isolated and protected computer. They are more complex to operate, but can capture much more information. For a detailed discussion about the different types of honeytraps and their relative merits, see: Lance Spitzner, Honeytraps – Tracking Hackers (2003).

Since the Honeypot is not connected to the production system, it creates no risk for the system.<sup>120</sup> In addition, since the Honeypot is not part of the legitimate system, accessing the Honeypot immediately alerts someone of unauthorized activity, or an intentional attempt to break into it. After all, no one but an attempting unauthorized user has any reason to search this system. The operator does not need to regularly monitor the Honeypot, and alerts only when an attempt for unauthorized access is made. In a sense it is the perfect trap: always-on, requires no human monitoring, alerts only when a suspect is caught, and does not trigger a plausible entrapment defense as it passively waits for predisposed criminals.

The Honeypot can serve for later prosecution, but often this is not its primary goal.<sup>121</sup> It mainly serves to collect information about patterns of attacks, follow trends in attacks, assess risk, and identify propagating attacks at an early stage. It aims at detection, early warning, prediction, and awareness. The ability to monitor and log attempts of unauthorized activities serves as an essential tool in prevention of future attacks.<sup>122</sup> The logs of the Honeypot can serve to “train” a predictive system to identify patterns of attacks, and to create “signature” of attacks for future defense systems. It can further help a company to identify the potential motive of attackers and assess the risk accordingly. Last, it is an essential instrument for the government and for companies who

---

<sup>120</sup> “Honeypots all share the same concept: a security resource that should not have any production or authorized activity. In other words, deployment of honeypots in the network should not affect critical network services and applications. A honeypot is a security resource whose value lies in being probed, attacked, or compromised.” (<http://www.honeypots.net/>).

<sup>121</sup> In prosecution of an attempted crime based on evidence collected from a Honeypot the defendant is likely to raise the entrapment doctrine. However, as we discussed earlier, with the current entrapment doctrine this claim is unlikely to succeed. See more: Ian Walden & Anne Flanagan, Honeypots: A Sticky Legal Landscape?, 29 Rutgers Computer & Technology Law Journal 317, 318 (2003).

<sup>122</sup> The literature about Honeypots normally differentiates between *Production Honeypots* and *Research Honeypots*. “The purpose of a production honeypot is to help mitigate risk in an organization. The honeypot adds value to the security measures of an organization.” Production Honeypots serve organization in their risk assessment and risk mitigation process. In comparison, Research Honeypots “included honeypots that are designed to gain information on the blackhat community. These honeypots do not add direct value to a specific organization; instead, they are used to gather intelligence on the general threats organizations may face, allowing the organization to better protect against those threats.” Lance Spitzner, The Value of Honeypots, Part One: Definitions and Values of Honeypots, SecurityFocus, October 10, 2001. Research honeypots serve the overall security community, as “they gather intelligence for entire communities and indirect benefits include improved attack prevention, detection and reaction.” Brian Scottberg, William Yurcik and David Doss, Internet Honeypots: Protection or Entrapment? IEEE International Symposium on Technology and Society, June 2002.

develop security tools. Since private companies are reluctant to report attacks on their systems, or provide real-time access to their logs, the government and security companies lack timely information. This information is necessary to assess risk, dynamically defend against a propagating attack, and develop new security tools. By deploying Honeypots, the government and private security companies can get timely information about the patterns and trends of attacks.<sup>123</sup>

Honeypots can get information and defend against many different crimes. Since every cybercrime is, in essence a communicative act, a Honeypot can be designed to attract various potential perpetrators to interact with it. It can serve, for example, to attract someone, who is interested in stealing trade secrets, to get access to seemingly confidential documents. In a recent case, it was used to track credit card fraud. A company “established an Apache Web site that presented fake Microsoft IIS Web server bug that supposedly exposed a file containing bogus credit card information. The company designed the trap to snare intruders who tried to steal the credit card data. The operation succeeded in catching thieves in the act of stealing the bogus data file”.<sup>124</sup> It can also, for example, attract spammers to use the system to route his unsolicited e-mails, then follow his activity.<sup>125</sup> Recently, Honeypots are being used to attract criminals who aim to remotely store illegal content or attack tools. The Honeypot appears to be a vulnerable system which can be easily compromised, and is therefore targeted by criminals. Once identified by the Honeypot, it can then track their activities and plans.

Recent scholars have indicated that Honeypots can also be used preemptively against identified attackers. Developers of Honeypots have demonstrated how to use it to disable an attack tool, retaliate against an attacker, patch security vulnerability within a system

---

<sup>123</sup> Brian Scottberg, William Yurcik and David Doss, Internet Honeypots: Protection or Entrapment? IEEE International Symposium on Technology and Society, June 2002.

<sup>124</sup> Mark Joseph Edwards, Honeypots with a Sting, Windows IT Pro (at: <http://www.wondowsitpro.com/Article/ArticleID/25679/25679.html>).

<sup>125</sup> See for example the Open Relay Honeypot, Jackpot (<http://jackpot.uk.net>).

that initiates a DDos attack, or send the attacker marked files which can later identify him.<sup>126</sup>

This method of marking a potential criminal for later identification has become a distinctive method of proactive undercover policing. It marks files or tools in the possession of users, which can then be used to associate them with criminal activity. Assume that a company wants to find who is spreading confidential information to external sources during litigation. They can send fake confidential information to many users within the company network, but mark each file with a unique fingerprint. If the confidential document is later presented in court, they can identify the internal source of the leakage. A similar mode of operation serves copyright owners to find illegal distributors of pre-release versions of movies or music discs. In these cases, the undercover element is the identifying mark that is embedded in the digital file which helps to identify a wrongdoer if he misuses the file.

Last, undercover operations have recently progressed and aim not only at potential criminals, but also at potential victims. Private entities and public authorities, such as the Securities and Exchange Commission (SEC), have set up bogus websites that follow a pattern of a known scam or fraudulent scheme. When a user falls into the trap, he is directed to a warning which educates him about falling prey to such a scheme. Mark Joseph Edwards covered such an operation in a recent column: “The Securities and Exchange Commission (SEC) posted a press release to lure investors to the Web site of McWhortle Enterprise, a fictitious company about to make its initial public offering (IPO) in the stock market. The company’s nonexistent product, the Bio-Hazard Detector, was a protection device that played on the public fears of terrorist attacks. The device claimed to detect ‘microscopic levels of hazardous bio-organisms... even the finest-milled, weapons-grade biohazards from 50 feet, long before the risk of inhalation or cutaneous (skin) infection, by testing for the distinctive surface leptins

---

<sup>126</sup> Laurent Oudot, Retaliation with Honeypot, Presentation at the 2004 Hackers on Planet Erath conference (HOPE 5) (at: <http://www.rstack.org/oudot/5th-hope/5thhope-oudot.pdf>).

(neurotransmitters).’ The company sought to raise millions of dollars and promised investors 400 percent gains in just 3 months. However, when visitors reached the fake McWhortle Web site, they were led to a warning page that said ‘If you respond to an investment idea like this... you could get scammed!’ The SEC, THE Federal Trade Commission (FTC), the North American Securities Administrators Association (NASSA), and the National Association of Securities Dealers (NASD) sponsored the operation, which was designed to make online investors more cautious to prevent online investment fraud from succeeding.”<sup>127</sup> This idea of using bogus sites to educate potential victims about potential scams is also currently being introduced in relation to other crimes.

These operations address the problem that we identified in Chapter One of users that still need to acquire the appropriate intuitions and awareness of cybercrimes. These traps aim at the victim and train him to recognize a suspicious pattern.

---

---

<sup>127</sup> Mark Joseph Edwards, Honeypots with a Sting, Windows IT Pro (at: <http://www.wondowsitpro.com/Article/ArticleID/25679/25679.html>).

---

### 3) Designing Crime Out

The new policing system is heavily dependent on crime-oriented design of the virtual environment. The designers of the new environment write the code, “the software and hardware that make cyberspace what it is”.<sup>128</sup> The design of the code endeavors to make crime impossible (“design crime out”) or at least reduce the opportunities for crime. It is a different design process than the traditional one of products, systems and services. Designers normally focused on making the product, system, or service “user friendly”. Other mechanisms in society – and mainly the criminal justice system - were called in to provide a solution for its misuse in criminal activities. The new designers are asked to anticipate the vulnerability of their product, system, or service to criminal use. They are instructed to make the code “abuser unfriendly”. The new designers are called upon to “incorporate crime prevention within their remit”.<sup>129</sup>

The new design process reflects a change in the mindset of code developers. In the new design environment, security considerations are introduced at the first stage of the design. Software is required to be “Secure by design”. “Creating secure software must start with a formal design process that verifies the security properties of the software at each stage of construction. For the process to work, designers and developers must be trained. There must be a process that comprehends the possible threats and designs around them.”<sup>130</sup> In this process, information security has changed its focus from better algorithms to protect information (e.g. encryption algorithms) to the social context and implementation of the code.

---

<sup>128</sup> Lawrence Lessig, *Code – and Other Laws of Cyberspace* (1999), 89.

<sup>129</sup> Paul Eklom, *Gearing Up Against Crime: A Dynamic Framework to Help Designers Keep up with the Adaptive Criminal in a Changing World*, *International Journal of Risk, Security and Crime Prevention*, Vol. 2/4 (October 1997) 249-265. (Eklom calls for this shift in thinking from “user friendly” to “abuser unfriendly”).

<sup>130</sup> David Acusmith, *The Digital Crime Scene: A Software Prospective* (at: [http://islandia.law.yale.edu/isp/digital%20cops/papers/aucsmith\\_newcrimescene.pdf](http://islandia.law.yale.edu/isp/digital%20cops/papers/aucsmith_newcrimescene.pdf)) (The author notes, however, that the traditionally software was developed with little consideration for security and there is still a need to train developers and designers to make this shift. “Unfortunately, there is much software developed without a clear design. As has been said, ‘Software developed without a functional specification can never be wrong. It can only be surprising’”).

Information security becomes more human-centric rather than technology-centric. Information security, which was traditionally the realm of mathematicians and engineers, gradually opens to social scientists.<sup>131</sup>

This shift in focus of information security occurred almost without a clear social theory or even conceptualization of a new mission. It is only recently that sociologists and criminologist are catching up with information security practices to examine them theoretically. But, if we apply modern theories of crime to information security, we may be surprised at the outcome. Security solutions, which were developed to solve particular problems, surprisingly position information security at the cutting edge of applied social theory. Information security follows the “opportunity theories” that focus on the role of opportunities in the decision to commit a crime. Unlike traditional criminology theories which were “theories of criminality and delinquency and not theories of crime”<sup>132</sup>, the new ones focus on the crime itself, the “interaction between disposition (to crime) and opportunity.”<sup>133</sup>

These *Opportunity Theories* inform the “applied criminology” theories of Crime Prevention through Design. The Theory of *Crime Prevention through Environmental Design* (CPTED) “is based on one simple idea – that crime results from the opportunities presented by physical environment. This being the case it should be possible to alter the physical environment so that crime is less likely to occur.”<sup>134</sup> This theory began with architectural studies, and is focused on the strategic design of buildings and urban

---

<sup>131</sup> Robert Willison & James Backhouse, Re-Conceptualizing IS Security: Insights from a Criminological Perspective, Department of Information Systems, London School of Economics and Political Science, Working Paper Series 132 (March 2005) (The authors speak of the “technical orientation” in conceptualizing information systems. “A direct consequence of the technical orientation is lack of social science theory both used and advocated by IS security academics. If IS risks are not simply reflections of information and communication technology (ICT) but are more intrinsically embedded in a ‘risk and technological culture’... then security research must find and apply social theory that can adequately address the dialectics of ICT and organizational security.”)

<sup>132</sup> Ronald V. Clarke, The Theory of Crime Prevention through Environmental Design (at: [http://www.e-docs.net/Resources/Articles/Clarke\\_the\\_theory\\_of\\_crime\\_prevention\\_through\\_environmental\\_design.pdf](http://www.e-docs.net/Resources/Articles/Clarke_the_theory_of_crime_prevention_through_environmental_design.pdf)).

<sup>133</sup> Ibid, there.

<sup>134</sup> Clarke, The Theory of Crime Prevention Through Environmental Design, Ibid.

planning to reduce opportunities of crime.<sup>135</sup> A supplementary theory developed to inform product designers called *Crime Reduction through Product Design* (CRPD). “[it] involves integrating protective features into products in order to reduce their potential to become targets of criminal activity (such as theft, fraud and damage), as well as preventing their use as instruments of crime.”<sup>136</sup>

In practice, code designers of the virtual environment follow these theories to reduce online crime. They are the new architects and designers of products (and services) of the new environment. These designers enjoy great flexibility, “As Lessig observes, the Internet, and artificial environment, is all architecture (or code) and thus infinitely malleable, at least in theory.”<sup>137</sup> The code both constrains and enables our activities in cyberspace. “This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned.”<sup>138</sup> In cyberspace, the opportunities for criminal behavior are controlled by the code. It is therefore being used strategically to prevent crime. Even if instructions and training for code writing often do not reference social theory, the emerging model of information security follows the logic and methods of these social design theories.<sup>139</sup>

---

<sup>135</sup> Neal Kumar Katyal, *Architecture as Crime Control*, 111 *Yale Law Journal* 1039 (2002) (Professor Katyal discusses four architectural concepts to control crime: “Increasing an area’s natural surveillance (its visibility and susceptibility to monitoring by private citizens), introducing territoriality (by demarcating private and semiprivate spaces), reducing social isolation, and protecting potential targets.” Professor Katyal then continues to discuss the strategic role of regulation through architecture that I will cover in a later section).

<sup>136</sup> Andrew Lester, *Crime Reduction through Product Design*, Australian Institute of Criminology, Series on Trends & Issues in Crime and Criminal Justice, Paper No. 206 (available at: <http://www.aic.gov.au>). See also an excellent collection of articles in the field that is to be published soon as a book: *Designing out Crime from Products and Systems*, Crime Prevention Studies, Vol. 18 (ed. Ronald V. Clarke & Graeme R. Newman) (TBP).

<sup>137</sup> Neal Kumar Katyal, *Architecture as Crime Control*, 111 *Yale Law Journal* 1039, 1041-1042 (2002). Dave Kumar discusses the practical limitations on the malleability of code that are presented due to *Network Effect*, *Path Dependency*, and *Lock-In effect*. See: Dave Kumar, *Problems with Code-Based Regulation* (at: [http://cyber.law.harvard.edu/fallsem98/final\\_papers/Kumar.html](http://cyber.law.harvard.edu/fallsem98/final_papers/Kumar.html)).

<sup>138</sup> Lawrence Lessig, *Code is Law – On Liberty in Cyberspace*, *Harvard Magazine*, January-February 2000.

<sup>139</sup> See for example the taxonomy for Anti-intrusion Techniques which follows information security literature, but can be similarly read as an applied document of the social theory of crime. The particular methods, that this technical document covers, are identical to those advocated by the manuals for applying social design theories for crime control. I will later discuss these particular methods. See: Lawrence R. Halme & R. Kenneth Bauer, *AINT Misbehaving: A Taxonomy of Anti-Intrusion Techniques*, SANS Intrusion Detection FAQ (at: <http://www.sans.org/resources/idfaq/aint.php>).

I will explicate the methodology of “designing crime out” through Code. However, to be able to better categorize it, and understand its effect, I will first briefly introduce the relevant theory of crime, *Situational Crime Prevention*. “Based on the premise that much crime is contextual and opportunistic, situational initiatives typically alter the context to diminish opportunities for crime. It does not aim to affect offenders’ propensities or motives. It takes these as given, and proceeding from an analysis of the circumstances giving rise to particular crimes, it introduces specific changes to influence the offenders’ decision or ability to commit these crimes at particular places and times. Thus it seeks to make criminal actions less attractive to offenders rather relying on detection, sanctions or reducing criminality through, for example, improvements in society or its institutions. This approach can be applied to any environment, product or service which is the potential target of crime.”<sup>140</sup>

The Situational Crime Prevention theory follows certain assumptions about criminal behavior, as explained by Newman and Clarke<sup>141</sup>: 1) Criminals act according to a model of rationale behavior. “That is, given their commitment to achieving the particular goal of their crime (e.g. robbery of a bank) they follow a rational course of action that will lead them to completion of that task”; 2) “Modifying a situation to make it more difficult to complete a criminal project is the logical response to criminal behavior”; 3) “Personal predispositions and other causes of crime (e.g. family history, race, heredity, social class) are relegated to a place of secondary importance in understanding crime. This is because they are viewed as (a) variables that are too abstract and non-specific... and (b) factors

---

<sup>140</sup> Design against Crime in Context, Extract from a report to the Home Office and the Department of Trade and Industry, UK, 2000, 10. Newman and Clarke summarized the situational crime prevention approach to include 4 elements: “1) It primarily seeks to solve crime problems in actionable setting... 2) Its methodology is to analyze and break down an identified crime problem into its specific parts... 3) Situations in which crimes occur are the focus on the study, for they demand specificity: they provide concrete clues to both the behavior of the criminals and how the environment (both social and physical) – as seen through the prism of the situation – may be changed to affect criminal behavior. 4) As an explanatory theory of crime it is unique in that it assumes the explicit value of preventing or reducing the identified crime problem.”, Graeme R. Newman & Ronald V. Clarke, *Superhighway Robbery – Preventing E-Commerce Crime* (2003) 7.

<sup>141</sup> Newman & Clarke, *Superhighway Robbery*, Ibid, at 8.

that are nor generally accessible to direct change, as are situations...”; 4) “The extent to which criminals can be prevented from carrying out their ‘mission’ depends on the strength of commitment that they have to completing their crime.” If the criminal is committed to it, he may find another way to displace the originally planned method of committing the crime (a.k.a. “*Displacement Effect*”).<sup>142</sup>

Accordingly, in order to reduce the opportunity of crime, this theory follows four main operational approaches: 1) Increasing the criminals’ *perceived effort* to commit the crime<sup>143</sup>; 2) Increasing the criminal’s *perceived risks* in committing the crime; 3) *Reducing anticipated awards*; 4) *Removing the excuses* for criminal behavior.<sup>144</sup> These approaches inform the primary design process. It translates into a new mindset that incorporates prevention strategies at the design board. Designers are called upon to think about how to *deter* crime (making it more risky), *discourage* it (making it harder, or less

---

<sup>142</sup> Marcus Felson & Ronald V. Clarke, *Opportunity Makes the Thief: Practical Theory for Crime Prevention*, Police Research Series Paper 98, Home Office Research, Development and Statistics Directorate (1998). The authors describe five different types of displacements of crime: *geographical displacement* (crime moves from one location to another); *temporal displacement* (crime moves to another time); *target displacement*; *tactical displacement* (substituting the method for committing the crime); *crime type displacement* (substitution for another crime). Many scholars have noted that it is just “common sense” to expect the displacement effect when the opportunity for a particular crime or a particular victim is reduced. Accordingly, they have critiqued crime prevention attempts as social waste if the crime is displaced by not prevented. However, recent research on the displacement effect shows that it is not as common as previously assumed. “Crime prevention initiatives can produce very substantial net gains, and commonly very little or no displacement is found. Reducing the local ‘pot of opportunity’ reduces crime”, Stephen Town, *Crime Displacement: the Perception, Problems, Evidence and Supporting Theory*, at [Crimereduction.gov.uk](http://Crimereduction.gov.uk).

<sup>143</sup> It is important to note that the theory focuses on the “perceived” effort to commit the crime (and the perceived risk) from the criminals’ perspective. In order to affect his behavior – assuming that he follows rationale behavior – we need to effect his perception of the effort/risk, while the “actual” effort or risk can divert from it. This implies that the actual effort or risk can be higher than the criminal perceives it, and in that case that crime may not be prevented. On the other hand, the actual effort or risk can be lower than the criminal perceives them, and therefore he will refrain from attempting to commit the crime. This leads to the conclusion that it may be worthwhile to manipulate the criminal’s perception to reduce crime, even if we cannot change the actual effort it takes to commit the crime or the risk that is associated with it. The virtual environment, since it is opaque, potentially opens many avenues in manipulating the criminal’s perception without actually changing the conditions for crime. Accordingly, Ekblom asks designers to distinguish “between mechanisms of *deterrence* (the preventive methods works by influencing the offender’s perceived risk of anticipated negative outcomes such as expenditures of effort and risk of arrest) and of enhancing *objective difficulty* (the method works by physically blocking the offence, necessitating more time to complete it or requiring more skill and equipment)”, Ekblom, *Gearing Up against Crime*, *Ibid.*

<sup>144</sup> Clarke in his work identifies 4 opportunity-reducing techniques for each strategy, making it 16 techniques altogether, see: Ronald V. Clarke, *Situational Prevention: Successful Case Studies* (1997).

rewarding), and *remove excuses* for it. In addition, they are requested to consider how to make the targets of the crime less vulnerable, less attractive for criminal, and also how to introduce new *Crime Preventers* into the environment, and how to remove *Crime Promoters* from the environment.<sup>145</sup> Recent literature has further elaborated on the particular design methods to achieve each one of these objectives.

In the physical environment, for example, an architect and a product designer can employ a handful of methods to achieve these goals.<sup>146</sup> Manuals for architects and product designers have become popular, and they cite plenty of methods, case studies and examples for successful crime prevention through design.<sup>147</sup> They recommend increasing the perceived effort of committing a crime such as burglary or theft by *Target Hardening* (e.g. locks), *Access Control* (e.g. fences or entry phone), or *Deflection* of offenders from targets (e.g. segregating fans in soccer stadiums). In addition, to increase the criminal's perceived risk, the designer can add *Detection Tools* into the environment (e.g. screening machines at the entrance), or *Surveillance Capabilities* (either by surveillance technology such as cameras, or by designing the space for *Natural Surveillance*). The design process can further support methods that reduce anticipated awards, such as *Target Removal* (e.g. replacement of cash operated phone with card operated phone), *Property Identification* (e.g. vehicles' marking), *Reducing Temptation* (e.g. gender-neutral listing on mailboxes), or *Benefit Denial* (e.g. ink merchandise tags). Last, the design can remove excuses for wrongdoing by *Alerting Conscience* (e.g. warning signs, such as "shoplifting is theft"), and *Facilitating Compliance* (e.g. easy checkout counter).<sup>148</sup>

---

<sup>145</sup> Design against Crime in Context, Extract from a report to the Home Office and the Department of Trade and Industry, UK, 2000, 10-11.

<sup>146</sup> See: Andrew Lester, Crime Reduction through Product Design, Australian Institute of Criminology, Series on Trends & Issues in Crime and Criminal Justice, Paper No. 206 (available at: <http://www.aic.gov.au>).

<sup>147</sup> See for example: Design against Crime in Context, Extract from a report to the Home Office and the Department of Trade and Industry, UK, 2000; Barry Poyner & W.H. Fawcett, Design for Inherent Security: Guidance for Non-Residential Buildings (1995); Dr Lorraine Gamman & Ben Hughes, "Thinking Thief" – Designing out Misuse, Abuse and 'Criminal' Aesthetics, *Ingenia* Issue 15, February – March 2003 (at: <http://www.raeng.org.uk/news/publications/ingenia/issue15/Gamman.pdf>).

<sup>148</sup> Recently new technologies and electronic devices are incorporated into products to increase their crime prevention capabilities, see: Peter Grabosky, Technology & Crime Control, Australian Institute of Criminology, Series on Trends & Issues in Crime and Criminal Justice, Paper No. 78 (at: <http://www.aic.gov.au>).

Information security employs all these methods in its attempt to proactively obstruct opportunities for crime.<sup>149</sup> Currently, these methods are employed simultaneously in Unified Information Security Systems to provide comprehensive design solutions. They tackle different types of crime, such as unauthorized use or fraud. A few years ago, the different components of a security system were normally employed and managed separately (e.g. intrusion detection, firewall, and honeypots). Now, these modules (or some of them) are commonly packaged together to create a synergetic effect between the modules, producing a single control interface for the user.

Each information security module embodies certain design principles, such as *Target Hardening* (e.g. encryption of files, vulnerabilities scanning, or intentional obstacles such as computation time<sup>150</sup>), *Access Control* (e.g. passwords and access control lists), *Deflection* (e.g. Honeypot), *Detection* (e.g. intrusion detection system or Honeypot), *Surveillance* (e.g. audit trails or keystroke loggers), *Alerting Conscience* (e.g. “Unauthorized use” warning), *Benefit Denial* (e.g. disabling illegally downloaded software), and *Property Identification* (e.g. watermarks and fingerprints). Working in tandem, these modules can produce *Defense in Depth*. They can further produce dynamic feedback between the different modules and enable a real time adaptive security operation. The intrusion detection system can, for example, identify anomalous use, then trigger an active change in access control rules, which would require further identification from the user. Alternatively, the detection of possible misuse can trigger a change in the surveillance mechanisms, such as keystroke logging for that particular user.

---

<sup>149</sup> See: Graeme Newman & Ronald V. Clarke, ETailing: New Opportunities for Crime, New Opportunities for Prevention, Foresight Crime Prevention Panel, February 2002. Professor Katyal in his article focuses on the use of certain architectural methods that are used in physical crime prevention, and can be employed online. He discusses how the designer of code can create opportunities for *Natural Surveillance*, *Sense of Territoriality*, *Build Communities* and *Harden Targets*. See: Katyal, Digital Architecture as Crime Control, Ibid.

<sup>150</sup> More about the intentional use of obstacles that aim to discourage certain potential attackers, see: Hamle & Bauer, AINT Misbehaving, Ibid.

Therefore, this dialogue between the security modules, and the adaptability of the environment makes the virtual environment unique. If, in the physical environment, the architecture or design of a product was fairly rigid, this is now not the case with the digital one. In the physical environment, the original design basically dictates the limitations of crime protection, and we have to live with ‘legacy’ failures in design.<sup>151</sup> Moreover, the physical design is not effective in adapting to new patterns of crime. Even if the original design was crime-aware and established certain features to prevent crime, they can become obsolete or irrelevant with a change in pattern of crime. Furthermore, the designer can only make a binary choice: to include the design features or not, even if these features could be useful in certain situations and for certain crimes, but undesired for others. It also creates a constant trade-off between functionality, aesthetics and security. To put it simply: a brick fence could be a wise design for crime reduction, but can also create an obstacle for the optimal use of the space, and further block the view.

However, the design of the digital environment for crime prevention enjoys a much greater flexibility and adaptability to changing circumstances. This is not to say that digital design doesn't experience any rigidity, but this rigidity is relatively limited in comparison with physical design.<sup>152</sup> It is also not to say that trade-offs between functionality, interface aesthetics and security are not apparent in this design.<sup>153</sup> There are trade-offs, but they can often be mitigated by operating the security device in the background (without effecting the aesthetics or user's experience) or by selectively employing it under certain specified conditions.

---

<sup>151</sup> Eklblom focuses on the concept of modularity which guides the design of computer systems, and asks designers to consider it also for physical objects to enable later upgrades. Modularity in physical product is however limited in comparison to digital “products”. See: Eklblom, *Gearing up against Crime*, Ibid.

<sup>152</sup> In theory, digital design is “infinitely malleable”. However, in practice, designers of code experience some rigidity due to original design decisions, dependency on “legacy systems”, and considerations of interoperability with other systems. Legal and ethical constraints can also limit the menu of design options that are available to the designer of code.

<sup>153</sup> These trade-offs often make designers prefer functionality and ease of use over security. Alternatively, the designers leave the decisions to the user; whether to prefer functionality and ease of use or security. For example “automated forms filler” in software that can save time by automatically filling rubrics, such as passwords and other identifying information. This feature makes use more convenient, but adds security risks from unauthorized users of the computers. The choice whether to enable or disable it is given to the user.

In general, we can say that the design of the virtual environment enjoys flexibility in three dimensions that are important in crime prevention: Personal, Situational and Evolutionary. By *Personal Flexibility*, I mean the ability to adjust the design to the particular user based on his risk profile. The system can dynamically assign different “Architectures” for different users; either to fit their particular needs or to mitigate their particular risk. The security system can, for example, erect a virtual fence for certain users where it would be an “open road” for others, or direct a particular user to a “Quarantined” system while others interact directly with the target system.<sup>154</sup> This Personalized Design also enables to actively change design decisions based on the user’s behavior or usage.<sup>155</sup> By *Situational Flexibility*, I refer to the ability of the system to dynamically make overall system design decisions in addressing changing risk conditions. Security systems can take “increasingly severe autonomous action if damaging system activity is recognized.”<sup>156</sup> The system can, for example, upon detection of potential attack, slow the system response, add obstacles or disconnect certain services from the network. *Evolutionary Flexibility* refers to the ability of the designer to upgrade the code based on an analysis of evolving security needs. The code is constantly changing to address newly detected crime patterns (e.g. added “crime signatures”), and the changing technological conditions of attack tools. This is a dynamic process of code evolution which progressively learns and anticipates potential new crimes and new crime patterns, and creates protective designs.<sup>157</sup>

---

<sup>154</sup> This adjustable and particularized nature of digital environment is best articulated by Larry Lessig in his book *Code and Other Laws of Cyberspace* (1999).

<sup>155</sup> Another variant of Personalized Design refers to the different treatment granted to human users and Bots (automated tools). As we discussed in Chapter One, cybercrime is often automated and security systems need to differentiate between a human user who interacts with the system, and automated tools which are potentially malicious. Therefore the system can set design features which enable the system to differentiate between a human and Bots, and therefore give them different responses (e.g. deny access only from the Bot). The system will differentiate between a human and a Bot normally by requesting to perform a task that is easy for a human to do, but hard for a computer to automatically do. The Access Control system can, for example, present a blurred word written in the shape of handwriting and ask to type the word. While a user can easily identify the written word, for a computer it would be hard to recognize the new pattern and identify the word.


<sup>156</sup> Halme and Bauer, *AIN'T Misbehaving*, Ibid. The system can either be programmed to automatically take “re-design” decisions or be redesigned with human operator’s decision.

<sup>157</sup> For discussion about the evolutionary dimension of design for crime prevention see: Paul Ekblom, *Gearing Up Against Crime: A Dynamic Framework to Help Designers Keep up with the Adaptive Criminal*

Further, it is important to note that information security design for protection mechanisms operate on various levels: file, application, system and network. It is also common to distinguish between protection measures which are designed for the client side and for the server side. With new technological protection measures, the scope of control expands to the user's machines; protecting the interests of owners or information subjects. In other words, the policing of access and use can shift to the location of use. For example, technological protection measures are set to protect copyrighted work. These technologies currently can control access to the work, control certain uses of the work (e.g. copying), protect its integrity, and can insure payment for access or use of the information.<sup>158</sup> Files can currently travel with unique identifying marks, and with rules for their use, and the technological protection measures at the user's end enforce these rules. This can be understood as *Mobile Policing* that can travel with the protected resource.

The sophisticated criminal may still use circumvention devices to bypass the technological protection measures. However, recent legislation, such as the Digital Millennium Copyright act prohibits the circumvention of technological protection measures. It further prohibits the development and distribution of circumventions devices and therefore creates legal obstacles for gaining the technology that is needed for circumvention. This legislation follows another method advocated by the situational crime prevention theory, controlling the *Facilitators of Crime* to reduce the opportunity for crime. As I mentioned in Chapter One, this new Anti-Circumvention legislation is highly contested (mainly due to its effect on the balance of copyright law and privacy implications of technological protection measures). Still, this legislation provides further incentive to use these technological protection measures to lock information, dictate the

---

in a Changing World, International Journal of Risk, Security and Crime Prevention, Vol. 2/4 (October 1997) 249-265; Paul Ekblom, Future Crime Prevention – a 'Mindset Kit' for the Seriously Foresight,  (March 2000) (at: [http://www.foresight.gov.uk/Previous\\_Rounds/Foresight\\_1999\\_2002/Crime\\_Prevention/Reports/future.htm](http://www.foresight.gov.uk/Previous_Rounds/Foresight_1999_2002/Crime_Prevention/Reports/future.htm)).

<sup>158</sup> See: J. Carlos Fernandez-Molina, Laws Against the Circumvention of Copyright Technological Protection, Journal of Documentation Vol. 59 No. 1 (2003) 41, at 43-45.

rules of use, and control access and use of information. It expands the trend that we have discussed to design out certain activities (either criminal or others).

