The engineer-criminologist and “the novelty of cybercrime”: a situated genealogical study of timesharing systems

Stefano De Paoli

The engineer-criminologist and "the novelty of cybercrime": a situated genealogical study of timesharing systems

Stefano De Paoli

Division of Sociology, Abertay University, Dundee, United Kingdom
Bell Street, Dundee, DD11HG, United Kingdom, s.depaoli@abertay.ac.uk

The Novelty of Cybercrime is a research problem in criminology where scholars are asking whether cybercrime is a wholly new form of crime compared with traditional-terrestrial crimes and whether new criminological theories are needed to understand it. Most criminological theories focus on the human rational aspects and downplay the role of non-humans in explaining what may be novel in cybercrime. This paper shows that a sociotechnical perspective can be developed for understanding the Novelty of Cybercrime using some insights from criminology. Working from the agnosticism principle of Actor-Network Theory and a situated genealogical perspective, it is possible to see that a criminological vocabulary can accommodate both the roles and relations of rational human and non-human actors. This is achieved by proposing the concept of the engineer-criminologist, developed by conducting a study of the development of information security for timesharing systems in the 1960s and 1970s. Timesharing security engineers were facing a completely new form of rule-breaking behaviour, that of unauthorised access and at the same time they were constantly using criminological concepts to shape their design of security and explain this behaviour. The concept of engineer-criminologists affords the use of criminological concepts in the sociotechnical study of the Novelty of Cybercrime.

Keywords: Novelty of Cybercrime, Actor-Network Theory, Situational Crime Prevention, malicious user, information security, engineer-criminologist

Introduction

Cybercrime is one of the phenomena defining our information age. There is however not an agreed definition and cybercrime is often seen as an umbrella term capturing a variety of activities (Wall, 2001), from cyber-pornography to serious data breaches. Different terms such as computer crime or Internet crime are also often used to address the very same phenomena. One accepted distinction is that between cyber-dependent and cyber-enabled crimes. The former are criminal activities which can only be conducted using “a computer, computer networks, or other form of ICT” (McGuire and Dowling, 2013, p. 5), for example malicious hacking. The latter are existing criminal activities that increase in scale “by the use of computers, computer networks or other ICT” (McGuire and Dowling, 2013, p. 5), for example frauds. The common denominator between the two is the conduction of criminal activities with computers and networks. For many years, criminology has offered reflections on whether cybercrime constitutes a novel form of crime, if compared to traditional-terrestrial crime. To take a simple example, are a fraud conducted face-to-face and one mediated by computers and the Internet the same or different phenomena? In other words: does the medium or the environment (computers and networks vs physical space) in which the fraud is committed change anything in terms of our understanding of said crime? In criminology, reflections about similar problems go under the name of the ‘Novelty of Cybercrime’ (NoC). The NoC is an umbrella term capturing whether new criminological approaches are needed to understand cybercrimes, or if approaches developed to understand traditional crimes are still tenable. Regardless of whether one supports new approaches or not, criminology remains subject-centric and the aetiology of crime remains the human criminal and her motivations, while the agency of non-humans is downplayed (van der Wagen and Pieters, 2015). This perspective excludes a-priori the possibility that it may be novel configurations of computers and networks – the non-human components of cybercrime – that configure completely novel roles for rational human criminals.

My core interest is not a criminological one. I am interested in the NoC from a sociotechnical perspective. This requires discussing some of the limits but also the potentials of criminological approaches. Rather than criticising criminology because of its subject-centricity and discarding its vocabulary, there is a much better avenue to follow. This paper proposes that the same conceptual vocabulary of some criminological perspectives can accommodate the study of sociotechnical interactions of humans and novel designs in relation to crimes committed with computer and networks. The criminological vocabulary is excellently suited for the study of crime phenomena and it can add much to a sociotechnical investigation of cybercrime. Moreover the adoption of this vocabulary within a sociotechnical ontology can facilitate a better dialogue between sociotechnical and criminological research.

My strategy for connecting a criminological vocabulary with a sociotechnical ontology requires shifting attention from criminology to focus on the work of information security engineers. Here, I follow an influential Science and Technology Studies (STS) perspective which has noted the scholarly tendency to "split the world up into separate technical and social systems rather than appreciate how engineers create and run sociotechnical systems" (Bijker, Huges, Pinch and Douglas, 2012, p. xxiii), and which seeks to avoid this split. There is debate on how to define information security due to a certain vagueness of some underpinning concepts (Anderson, 2003) and the unclear differences with the notion of cybersecurity (Voin Solms and Niekerk, 2013). In this paper I adopt a definition that was proposed in the context of timesharing systems (the case study proposed in this paper), where security was denoting "mechanisms and techniques that control who may use or modify the computer or the information stored in it" (Saltzer and Schroeder, 1975, p. 1279). Information security and criminology (of cybercrime) mostly deal with the same research object: crime and rule-breaking behaviour committed with computers and electronic networks. For criminology, the problem is to analyse the root human causes of criminal behaviour. Information security instead focuses on engineering mechanisms for protection of a system against criminal or deviant behaviour, while at the same ensuring the smooth conduction of rule-abiding behaviour.

Using an STS historical perspective, in this paper I will develop the novel concept of the engineer-criminologist in order to show how in information security engineering certain rule-breaking behaviours are identified, defined and materially addressed through what look very much like criminological concepts. At the same time security engineers – differently from criminologists – keep the social and the technical together in a sociotechnical system. To prove these points, I will present an historical case study research on the development of security for a family of computer installations know as timesharing developed in the 1960s and 1970s. Data for this study comes from scientific publications on timesharing security. For the analysis, I couple a genealogical approach (Foucault, 1972; Parikka, 2007) with the principle of theoretical agnosticism from Actor-Network Theory (ANT) (Callon, 1984 and 1987).

Due to the innovative networked and multiuser nature of timesharing systems, engineers had to face a completely novel form of rule-breaking behaviour[1]: unauthorised access to computer resources, done by an emerging criminal actor, the malicious user. Thus engineers working on timesharing were the first to deal with this

[1] I am avoiding using the word crime explicitly here because the kinds of behaviours in question were only codified as crimes decades later with the development of computer law, e.g. the Computer Fraud and Abuse Act (1986) in the USA.

novel form of rule-breaking behaviour emerging from a new configuration of computers and networks. This is an excellent NoC case study that will support the initial development of the notion of the engineer-criminologist, showing that timesharing engineers were using concepts very similar to a criminological approach known as Situational Crime Prevention (SCP) and that these concepts did allow them to explain the roles of criminal humans and technologies simultaneously.

The novelty of cybercrime

I will now consider a number of criminological contributions related with the NoC. Some deploy the metaphors "old and new wine" to categorise whether cybercrime is the same as traditional crime or something new. Much of this literature also relates with an influential theory known as Routine Activity Theory (RAT) (Cohen and Felson, 1979). I also include the only criminological publication which I found that considers the role of technology (van der Wagen and Pieters, 2015) openly critiquing RAT views on the NoC.

RAT authors, in general criminology, theorise that the "opportunity makes the thief" (Felson and Clarke, 1998) where nearly anyone presented with an opportunity to commit a crime (C) will do so, even righteous citizens. This opportunity is exploited by motivated offenders (O) when there is a suitable target (T) (e.g. a person, an object like a car or a place like a house) and the absence of capable guardians (G) (e.g. policemen or home owners) able to prevent the offender in exploiting the target. This is summarised with the formula O+T-G=C (Cohen and Felson, 1979). RAT considers crime from the perspective of the offender's bounded rational understanding of the situation. RAT is also concerned with a description of the target from the offender perspective using, for example, the VIVA model – to describe the Value (how the offender values the target), Inertia (how the offender sees the limits of moving a target e.g. it's weight, size), Visibility (e.g. is it in plain view or away from it) and Access (e.g. the target is fenced or locked away or easily accessible by anyone) (Cohen and Felson, 1979).

The issue of whether new criminological theory is needed to explicate the NoC has been categorised with labels such as transformationists or continuists by Leukfeldt and Yar (2016). This debate started when an influential continuist position was advanced by Grabosky (2001), for which it is possible to apply the RAT formula to the study of cybercrime. He argued that although on the surface we may see differences between cyber and traditional crimes, the motives driving criminals do not change: technology changes but human nature does not. A fraud – cyber or not – can still be explained as having financial strain as a motivation. Other cybercrimes, like traditional crimes, are motivated by greed or lust. For Grabosky cybercrime is "old wine in a new bottle".

Wall (1999) proposed that cybercrime is comparable to a "new wine", not contained by any physical space ("no bottles") and whose meanings shifts when moving from terrestrial contexts to cyberspace. Yar (2005) testing the RAT formula for the study of cybercrime also compared cybercrime to "old wine in no bottles". According to Yar, since the Internet changes the spatio-temporality of the situation, informational targets are always available to anyone connected to the network(s) and the offenders' capacity to commit crimes is not limited by space or time. For him, inertia of a target also does not apply as information is not weighted down by bulk if compared to physical targets. Informational targets instead still have value for criminals. Thus, for Yar, only some aspects of the VIVA model are applicable and criminology needs to reconsider existing theories.

Holt, Bossler and Siegfrid-Spellar (2015) reviewed a number of approaches showing that criminologists have largely used existing theories to study cybercrime. The authors also consider that cybercrime presents “instances of new wine” in relation to certain technological components, such as malware. While a parallel between traditional and cyber-frauds may be easily drawn, it is more difficult to compare malware to other terrestrial crimes. The same authors used RAT (Bossler and Holt, 2009; Holt and Bossler, 2013) to study the only remaining rational human component of the crime situation: the victims’ rational decision-making (e.g. whether victims update their anti-virus) which could lead to malware victimisation.

van der Wagen and Pieters (2015) focused on malware agency, noticing that much criminology does overlook the role of technology in favour of human-centric explanations and relegates technology as either a tool in the hands of a motivated offender or just as a background element of crime. The authors used ANT standard vocabulary, with concepts such as translation or hybrids, to study botnets, network of malware infected computers used for criminal activities such as Distributed Denial of Service. The authors argue that with a botnet, criminal agency is hybrid and not fixed once and for all, but shifts alongside the process of creation of a criminal technical infrastructure.

Analytical Perspective

The NoC notion seems to point to an evident technological component, together with a social/human one. In criminology we have however limited scholarship which considers a symmetrical treatment of humans and non-humans. In the introduction, I observed that criminologists are not the only scholars dealing with cybercrime. Another discipline is information security. This paper focuses on how information security engineers define what in RAT approaches is considered the crime situation. A first interesting aspect to note is that in criminological publications, information security is often relegated to a few lines, vaguely noticing that this is part of the guardian in the RAT formula (Grabosky, 2001; Yar, 2005), that it deals with the technical side of things (Bossler and Holt, 2009), that technical guardianship has almost no effect in reducing victimisation (Leukfeldt and Yar, 2016). These claims obscure some important aspects. Information security focuses on creating mechanisms for preventing unauthorised access and subsequent illegal or rule-breaking use of computing and network resources. Ensuring that information is not exposed to unauthorised parties requires not exposing informational targets to motivated offenders, located inside (so called insider threats) or outside an organisation. The focuses of criminology (of cybercrime) and information security largely overlap, with the latter focussing on the design of secure systems and the former on understanding the criminal. I propose to conduct an historical-genealogical study of information security for reconsidering some aspects of the NoC and propose a new concept.

I undertake research on the development of security for the timesharing systems which happened in the late sixties and early seventies of last century. Timesharing systems were the first to present innovations such as networked communication and multiuser computers. In that period, the networked transmission of communication came with the anxiety that previously established borders were becoming trespassed (Parikka, 2007). Timesharing engineers had to face for the first time novel forms of rule-breaking behaviour such as unauthorised access to information, destruction of content and denial of service (Saltzer and Schroeder, 1975). The notion of the user acting with malicious/criminal intent was formulated in association to timesharing for the first time (Anderson, 1972).

We can learn much about the NoC if we adopt a genealogical approach to information security and to the case of timesharing. Genealogy aims to account for the historical constitution of discursive practices and for the conditions of existence for truth and meaning in those practices (Foucault, 1972). Genealogy is a non-subject centric historical perspective and archaeology is the method of such history. Parikka (2007, p. XXXII), explicitly citing Foucault (2000), pointed that the function of (media) archaeology is to look at the immanent strategies producing reality and the goal for the analyst is to rediscover the connections of facts that at a given moment establish what subsequently counts as being self-evident, universal and necessary.

The approach I follow is more modest than those of Foucault and Parikka. For instance, Parikka conducted the archaeology of digital contagions over several decades, across different media, from scientific publications, to science fiction books to movies. My starting point comes from Actor-Network Theory, in which we can conceptualize an archaeological approach where the processes through which knowledge becomes stable are localised, for example at the level of a laboratory (Law, 2004).

I start from the theoretical agnosticism principle of ANT (Callon, 1984) which states that theories should not be used a-prioristically on phenomena. This principle acknowledges the importance of following social actors' production of methods for creating social order. I use this principle as the basis for the genealogical study of timesharing security. A narrow interpretation of this principle would lead to using the original ANT vocabulary, with concepts such as inscription or translation. However, this vocabulary is not prescriptive, just convenient (Latour and Akirch, 1992). When presenting my analysis, I will use a criminological vocabulary while respecting the theoretical agnosticism.

In a seminal paper, Callon (1987) applied the agnosticism principle to the case study of the development of an electric car in France, showing that:

> engineers who elaborate a new technology as well as all those who participate at one time or another in its design, development and diffusion constantly construct hypothesis and forms of argument that pull these participants into the field of sociological analysis. Whether they want it or not, they are transformed into sociologists, or what I call engineer-sociologists.

Callon showed that two different groups of engineers came up with competing visions about the role of the electric car in the French society, visions which Callon recognised as being similar to theories formulated by two known sociologists, Bourdieu and Touraine. One interpretation about structural changes in consumption (an implicit Bourdieusian view) was embraced by engineers at Electricité De France (the company sponsoring the car). An opposite view was embraced by engineers at Renault tasked with manufacturing the car. At some time in the project, the Renault engineers postulated that no changes would occur to consumption patterns (an implicit Tourainian view) and that the electric car would fail. By making the car (or making it failing) these engineers were at once designing a technological innovation and its social environment. From this insight, I then propose that as much as we have engineer-sociologists we may have information security engineers as criminologists. In other words, in information security the aetiological explanation of cybercrime may be accompanied and become a justification of design processes, whereby engineer-criminologists simultaneously design solutions for preventing crime and use constructs similar to criminology for explaining their crime prevention strategies. It is with the concept of the engineer-criminologist that I connect a criminological vocabulary – traditionally subject-centric – with the non-human aspects of computer and networks.

My data is a textual corpus derived from a range of relevant publications from the core period of development of timesharing protection (1965 to 1975), which have been retrieved with a search in scholarly databases. I selected a total of 22 documents suitable for my research (see Sources in References section), amounting to over 500 pages analysed. Most are research papers (e.g. Saltzer and Schroeder, 1975; Ware, 1967a), some are technical reports (e.g. Anderson, 1972; Parker, 1973a) and others are reflective papers on timesharing and societal changes (e.g. Baran, 1965).

The security engineer as criminologist

Timesharing systems were being hypothesised as early as the 1955 as a type of "operating system that permits each user of a computer to behave as though he were in sole control of a computer" (McCarthy, 1983). Computer installations were at the time expensive and available mostly in large Universities, large companies and military bases. They were a unique large mainframe operated as batch processing. Programmers would create their programs first (for example on punched cards) and then these were collected and executed in batches on the mainframe by a technician who would then report back the results (see Silberschatz, Galvin and Gagne, 2004, Chapter 22). This approach would not permit direct access to programming for programmers, leading to long waiting times for results. In time, it became clear that computational resources were not used optimally. Security was also largely a problem of shielding the mainframe from unauthorised outside physical access, where only authorised technicians had cleared access (Parikka, 2007).

Timesharing is a radically different concept where resources (especially Central Processing Unit's time and memory), e.g. for executing programs, are shared among a number of users connecting using remote dummy terminals (Figure 1). Timesharing allows direct and interactive access to programming and multiple users and computer programs share the computer resources at any one time (Silberschatz et al., 2004). Further, as users interact with terminals, timesharing included novel issues related to the exchange of data over networks. Terminals could be located within the same building as the mainframe but also in remote organisations. Thus, compared to batch programming, with timesharing we have a novel reconfiguration of technologies (mainframes connected to networks of terminals) and people (users with direct programming access). While the mainframe would still need to be physically protected, direct programming access posed new security problems:

> This "sheltered" approach promotes one-at-a-time, batch usage of the facility. Modern hardware and software technology has moved forward to more powerful and cost/effective time-shared, multi-access, multiprogrammed systems. However, three features of such systems pose a challenge to the sheltered mode of protection: (1) concurrent multiple users with different access rights operating remote from the shielded room; (2) multiple programs with different access rights co-resident in memory; and (3) multiple files of different data sensitivities simultaneously accessible. (Weissman 1969, p. 120)

Interestingly in the early years, some timesharing systems were built without security and this was only added as a post hoc development. These were defined as:

> Unprotected systems: Some systems have no provision for preventing a determined user from having access to every piece of information stored in the system (Saltzer and Schroeder, 1975, p. 1280)

Many security issues – or better protection as it was called at the time – arose in an emergent manner as outcomes of the design of functional timesharing systems, where there was a need to protect users from each other and to protect the mainframe from users and programs accessing resources.

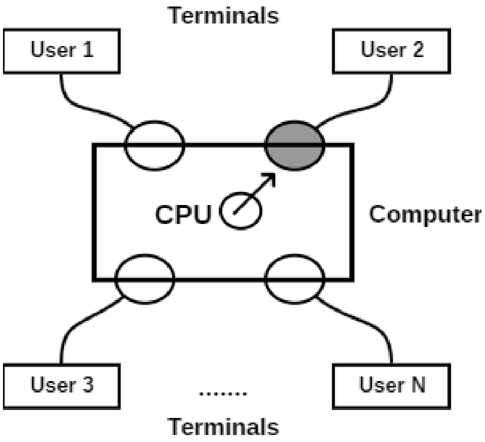

Figure 1. Timesharing: multiple users sharing computing resources via remote terminals.

In timesharing, data files, software libraries, user programs, computer memory and the operating system are all located and/or executed on the mainframe. In a timesharing system with no protection, any user could in principle access or manipulate any of those resources. Thus, by accident, a user could read the private files of another user, or even delete them (unauthorised access). A user could also accidentally crash the entire system by running faulty programs (denial of service). This is where the need to create protection among users and between users and the mainframe emerged. While protection was needed because of potential accidental actions, it became clear that those same actions could also be conducted with explicit malicious intent. Engineers were thus facing a completely novel form of rule-breaking behaviour, emerging from a new configuration of technologies and people. This was explained in the shift from single user to multi-user computers:

> Present day computer systems are largely closed use systems; that is, systems serving a homogeneously cleared user population. The major threat to these systems is that of external penetration. […] In effect, the defense against external penetration surrounds the system and its user community with a barrier that must be breached before the system can be compromised. (Anderson, 1972, p. 1)

In the batch configuration, the main risk thus comes from external penetrations, countered by a barrier composed of physical, procedural and communication techniques. On the contrary:

> The *malicious user* concept arises from the requirements for open use systems. […] By this we recognize that the nature of shared use multilevel computer systems present to a malicious user a *unique opportunity* for attempting to subvert through programming the mechanism upon which security depends (i. e. *the control of the computer vested in the operating system*). This threat, coupled with the concentration of the application (data, control system, etc.) in one place (the computer system) makes computers a *uniquely attractive target* for malicious (hostile) action. (Anderson, 1972, p. 3)

In this fundamental statement, Anderson argues that the malicious user emerges with the new requirements for timesharing systems, which afford direct programming access via networked terminals coupled with a concentration of resources. In the context of batch installations the malicious user is not a criminal category per se as the users are a security cleared population. The malicious user is instead someone operating within the perimeter of a timesharing system (Anderson, 1972: 58):

> It is given therefore that a hostile third party has direct programming access to a targeted computing system. It is the direct programming access to a computer system that constitutes the principal security threat.

Properties of this completely novel threat to computer systems are then emerging together with the very same design of systems that can be programmed directly. Anderson explicitly says that there is a new “opportunity” (emphasis in italics added) coming from the coupling of a potential malicious offender and an attractive “target” (emphasis added), multiuser timesharing. This terminology matches that of RAT and is used similarly, highlighting the work of what I call engineer-criminologists.

Situational Crime Prevention and the engineer-criminologists

An influential extension of RAT is known as Situational Crime Prevention (SCP), an approach originally developed in the late seventies and early eighties of the last century (Clarke, 1980). By using theoretical agnosticism, it is possible to see that engineers working on timesharing security were conceptualising their work in a manner very similar with how SCP scholars see the criminal situation. In an open critique of what he calls “modern criminology” Clarke (1997), the main author behind SCP, argues that SCP differs in two ways from much criminology. The first deviation is the focus on the crime situation rather on the criminal. Most criminology does not consider that the rational offender acts in a situation where opportunities emerge and will instead concentrate on which specific individual traits and social influences lead to crime. Crime is an emergent property of the situation where rational actors (the crime aetiology) take advantage of opportunities coming from the availability of targets and the absence of guardians (Clarke, 1997). There is a second critique to “modern criminology” which Clarke (1997) advances: that much emphasis has been placed on abstract measures for controlling the offender, rather than on modifying specific situations to prevent crime. Clarke mentions legislation and morality as abstract control measures. The increase of punishments in legislations is an example. An offender presented with an opportunity to commit a crime will likely take that opportunity without thinking much about abstract laws. SCP promotes instead the modification of the situation in order to reduce crime opportunities. Therefore SCP argues that formal and informal controls divert view from more efficient ways of control: the "routine precautions" which impact the behaviour of the potential offender.

If we look back at the statement by Anderson (1972) quoted in the previous section, he was using nearly the same vocabulary as SCP and RAT, except that no prevalence is given to the role of the offender. For Anderson, the opportunity is the sociotechnical articulation of design and people: a "new criminal" (the malicious user) emerges as outcome of a technological innovation (from batch to Timesharing) and from the presence of a technological guardian (control mechanisms) which may fail. Nowadays, this novel threat is known as the insider threat, the user that within the perimeter of an organisation commits criminal acts.

Timesharing engineers were thus facing similar problems to SCP scholars. We can consider the anticipated situation in which functional timesharing systems were designed without protection, and ask whether legislation would suffice to ensure order. Baran (1965) presented an analogy between rule-breaking behaviours in timesharing and the increase in obscene phone calls at the time, discussing that the response to obscene calls from authorities was that of increasing the penalties:

> It is a rare event when person making an obscene telephone call is caught, so the deterrent effect is almost nil. But an increased penalty hidden in a law book is the standard legal response to a basically technological/social problem. This writer would prefer to see technology which created this problem be required to provide more effective safeguards. (Baran, 1965, p. 49)

The writer makes it clear that it may be preferable to turn to the practical engineering of security than to penalties for addressing problems which are at once social and technical:

> each telephone (or at least those plagued with these calls) should have a button which when pressed bridges the call to a bank of recorders at the police station and a teletypewriter message with the name, address, and telephone number of the calling party transmitted to the nearest police car. It wouldn't take long to clean up the undesired callers. (Baran, 1965, p. 49)

The writer argues that telephones should have a button that the victim could use to report obscene callers and that this would be more effective than penalties. By extension of the analogy, order in timesharing should be created with designed solutions rather than with legislation and then:

> a wonderful opportunity awaits the computer engineer to exercise a new form of social responsibility (Baran, 1965, p. 49)

We have engineers offering a situational criminological perspective on the novel threat of the malicious user of timesharing. They offer a sociotechnical view on the crime opportunity, criminals, targets and guardians. There is a focus on defining the opportunity for a criminal action and the need for counteracting this action. Solutions to crime cannot come from formal controls on the offenders (penalties, criminal justice), but from engineering technical guardians. There also is recognition of the new social responsibility of engineer-criminologists: that of enabling social order.

Defining threats and countermeasures

Engineer-criminologists' main task was that of designing a technologically capable guardian. Browne (1972, p. 3), citing Sorensen (1972), defines the design of security/protection as a trade-off:

> the tradeoffs of cost vs. efficiency are of great importance. It is quite easy (and expensive) to put a lead wall around a computer system, thus insuring absolute protection. Of course no one can get any jobs through either. The key factors are to determine the value of information, then quantify the effect of having it lost, stolen, or destroyed. Then the cost of implementing protection can be weighed against the cost of loss

The process requires: (1) assessing the computer installation for risks related to theft and other hazards; (2) evaluating the security measures needed to protect the computer; (3) evaluating each measure in relation to the risk and costs, before deciding. This cost-benefit approach nowadays goes by the name of information technology threat/risk assessment (Bayne, 2002). Ware (1967, p. 288) remarked that this economical-rational principle of designing protection seems, conversely, to drive malicious users:

> In the end, an engineering trade-off question must be assessed. The value of private information to an outsider[2] will determine the resources he is willing to expend to acquire it. In turn, the value of the information to its owner is related to what he is willing to pay to protect it. […] Perhaps this game-like situation can be played out to arrive at a rational basis for establishing the level of protection.

[2] Here "outsider" refers to someone outside another user's private information within a system.

Engineer-criminologists conceptualised the criminal as a rational actor, like criminologists. Assessing the value of information for an offender (like in the VIVA model) and the possible threats in a rational manner is a precondition for a design which can mitigate the threats within the boundaries of available resources. Design of protection, which is a process for reducing crime opportunities, is about understanding the situation and potential threats before making an intervention.

Security engineers categorised the threats to information under three main areas (Anderson, 1972), still used today:

(1) Unauthorized information release.

(2) Unauthorized information modification.

(3) Unauthorized denial of use.

Where, clarify Salzer and Schroeder (1975, p. 1280):

> The term "unauthorized" in the three categories listed above means that release, modification, or denial of use occurs contrary to the desire of the person who controls the information, possibly even contrary to the constraints supposedly enforced by the system.

Again, we see an emphasis on the need to understand the target not just from the angle of the offender but also of the owner and even of the technical guardian. Anderson (1972) notes further that the tripartite distinction of threats does not provide the basis for design. Thus, engineer-criminologists devised top-down and bottom-up approaches. Top down approaches depart from a formalised model about a secure system and then protection requirements will follow (Lampson, 1974). Bottom-up approaches start by "identifying insights by studying example systems" (Saltzer and Schroeder, 1975, p. 1283). This part of the analysis is empirical and studies real systems and incidents before deciding which protection measures to implement. This analysis appears similar to the SCP approach for reducing the crime opportunities in specific situations.

Countermeasures and Opportunity-Reducing Techniques

Clarke (1997) emphasises that SCP is driven by action-research in order to devise solutions, whereby the routine activities of people are modified for reducing the opportunities of crime. An example related to the reduction of property crimes is what "the Post Office did when they virtually eliminated theft from telephone kiosks by replacing the vulnerable aluminium coin boxes with much stronger steel ones" (Clarke, 1980, p. 141). This amounts to hardening the crime target in the eyes of criminals. Another example relates to the fact that "apartment blocks with doormen are less vulnerable to burglary" (Clarke, 1980, p. 142); that is, a guardian brings increased risks for the offender. SCP seeks to make an intervention on a potential crime situation where criminologists, first understand what would constitute an opportunity for the rational criminal (e.g. the aluminium box) and then modify the target (e.g. a steel box) to reduce the opportunity. The SCP approach is based on the collection of data about specific crimes, an analysis of the conditions that permit crime, a study of possible countermeasures also based on rational cost evaluation, before the implementation of measures (Clarke, 1997).

The bottom-up approach to threat analysis presents nearly the same traits. Engineering security requires rational decision making and empirical research focussed on understanding how much the offender is willing to go to access a resource as well as how much the owner is willing to invest in security. Parker (1973b, p. 5), writing about the empirical approach to threat analysis, noted that:

> Real cases are superior to theoretical penetration exercises in some ways because they are occurring more frequently, they embody rational as well as unpredictable human behavior under natural stress, and they occur in real, undisturbed environments. Theoretical exercises are superior to real cases by being able to test specific security features under rigorous conditions in experimental systems.

Empirical research is useful to understand human behaviour which may be rational but also unpredictable and for the identification of threats based on these behaviours. Anderson (1972, p. 22) also explains that:

> The technical threat in contemporary systems posed by a malicious user is that because the systems are produced using ad hoc security rules, a penetrator will find a design or implementation flaw, or induce a 'trap door' situation to obtain supervisory control of the system.

Threats come from flaws in the ad hoc design of timesharing and direct programming access to the system by the potential perpetrator. For example, a trap door is an undocumented feature of a computer system, inserted on purpose by a potentially malicious programmer, which is not properly controlled. Often trap doors are inserted during the development of the operating system itself, or by exploiting software flaws for example in operating system registers, or even inserting the trap door in the software compiler of the operating system (see for an overview Karger and Schell, 1974). A trap door would allow the malicious programmer to take control of the entire system, in supervisor mode (Anderson, 1972).

Design flaws which can be exploited with direct programming are what in today’s information security vocabulary are called *vulnerabilities*. Writers at the time did detail a number of further explicit threats. There is not enough space here to see these in details, but many are common in contemporary Internet and computer systems, for example trojan horses (Anderson, 1972), masquerading (e.g. a terminal) as something else to steal information (Saltzer and Schroeder, 1975), and man in the middle attacks (Petersen and Turn, 1967).

Data collection on threats and analysis of the situation for a computer installation lead to the design of *countermeasures*, procedures and techniques to mitigate threats. The concept of countermeasures resembles what in SCP are called Opportunity-Reducing Techniques (ORTs) (see for an overview Clarke, 1997). Since the problem is to study the situation and intervene in modifying it when there are potential crime opportunities, SCP scholars have identified a number of heuristic techniques to guide practical interventions. SCP scholars can deploy one or more of the 25 ORTs that have been formalised to modify the situation and reduce crime opportunity. Although there is not enough space here to describe these ORTs in full, we have already touched upon some examples: hardening the target (e.g. a steel box rather than an aluminium one) or introducing a guardian (e.g. the doorman). Returning to timesharing, Turn and Petersen (1970, p. 4) defined the objectives of countermeasures as would any criminologists working with ORTs:

> The objective is not absolute security -this can never be achieved, but rather an increase of the cost of penetration, the "work factor', to a level where the expected payoff becomes relatively small. At the same time, a balance must be maintained between the cost of countermeasures and the value of the protected information.

Protection is very much about increasing the cost for crime perpetration (for example by hardening the target), while adopting a rational trade-off on costs. Saltzer and Schroeder

(1975, p. 1284) summarised the situation of protecting the target with an explanatory metaphor:

> Conceptually, then, it is necessary to build an impenetrable wall around each distinct object that warrants separate protection, construct a door in the wall through which access can be obtained, and post a guard at the door to control its use.

Protection countermeasures primarily focus on authentication (the technical guard identifies the user with something e.g. a password, to avoid exploitation of flaws) and access control (the engineer constructs a “door” which permits direct programming when authorised). These countermeasures are techniques which we can recognise also in SCP ORTs, where authentication matches a technique called “screen exits” and access control equates to the technique “access control of facilities”, both under what SCP scholars call “Increasing the Effort” (for the perpetration of a crime). Engineer-criminologists also considered a range of other countermeasures, though there is no space to consider them all here.

Symmetrical countermesures

To illustrate authentication and access control we can consider the Graham–Denning model (1972) as an interesting example of how timesharing engineers did anticipate with design solutions rule-breaking behaviours, while at the same time allowing legitimate programming of the system. These authors observed that security could be conceptualised in a model with three factors: a subject, an object and a set of rules enforced by a special operating system program called ‘monitor’. Rules relate to the capacity to create and delete subjects (e.g. computer admins creating new user credentials) and objects (e.g. user creating data files, software or memory locations) as well as giving subjects the capacity to access objects.

I want to emphasise here the resonance with another SCP claim that “situational prevention does not draw hard distinctions between criminals and others” (Clarke, 1997, p. 4). We can recognise a form of symmetry in this and a degree of agnosticism: in SCP no a-priori distinction is made between who is criminal and who is not. Criminals and non-criminals emerge from the situation.

Also in the Graham–Denning model no distinction is made a-priori between criminals and others. The goal is to devise countermeasures (protection, via the monitor operation) to facilitate a rule-abiding access that subjects can make to objects. The protection must also be capable of ensuring that no unauthorised access (accidental or not) will take place. In simplified terms, we may consider two subjects, Bob and Alice and two objects (File 1 and File2) on which different levels of access are established. For instance, Alice can both read and modify File 1 but Bob can only read File1, whereas for File2 Alice can only read this object and Bob has no access at all. This situation can be then mapped onto what in security is called an Access Control Matrix (Table 1).

	File 1	**File 2**
Bob	Read	<no access>
Alice	Read, Write	Read

Table 1. Simple access control matrix with two subjects

Thus, if Bob (a subject) attempts to write on File1 (an object) - whether incidentally or maliciously - the monitor enforces access control and prevents Bob from doing that. Bob may indeed be attempting to modify a register of the system in order to place a trap door, but he may just be trying to access the file incidentally. However, the model implementation does not need to decide a-priori whether Bob is a criminal or not: it just prevents him accessing a critical part of the system. The symmetry postulated by SCP is used also by engineer-criminologists where their model does not distinguish a-priori between criminals and others. Furthermore, we have observed earlier the difficulties that much of criminology has in reconciling subject-centric theorisation with malicious non-human software. In the Graham–Denning model, a subject may be a user but also a process, whereby a process is an active computer program (e.g. a program using a software library available as a service on the system). The model proposed by engineer-criminologists does not distinguish a-priori whether it is a human-subject or a program-subject conducting an action on an object like a file. This is a second symmetry of the model. Interestingly there is a third symmetry in the model, namely that no a-priori distinction is made on whether a process/program is malicious or not.

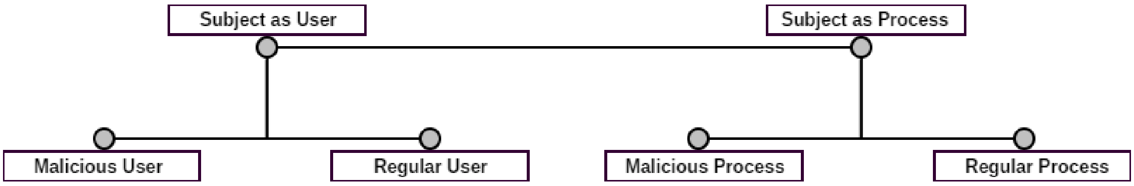

Figure 2. The three symmetries of the Denning-Graham model

If in the Access Control Matrix (Table 1) we replace Bob and Alice with Process1 and Process2 and we have Process1 trying to modify the File1 (e.g. accessing a software library trying to alter it by e.g. implanting a back boor), then the monitor will not open a door giving access to the object/resource. This will prevent a potential rule-breaking behaviour by potentially malicious software. Again, whether a software is malicious or not is an emerging outcome of the situation.

Discussion and Conclusion

The contribution of this paper was to better understand what in criminology is defined as the Novelty of Cybercrime and start developing a sociotechnical approach to it. Criminology is traditionally subject-centric and regardless of whether it perceives or not novelties in cybercrime phenomena, it still sees the rational human criminal as explanatory factor of a crime. While this approach is justifiable from a disciplinary perspective, it limits our capacity to fully grasp the situational and emergent sociotechnical aspects of a cybercrime opportunity. van der Wagen and Pieters (2015) are right in noticing that most approaches in criminology attribute all the weight of a crime to humans. Consequently, we inevitably fall into investigation about motives, while overlooking aspects of technological agencies. In criminology, it remains difficult however to make room for approaches addressing the NoC which can treat symmetrically humans and nonhumans and for alternative vocabularies like those proposed by ANT. Instead, the criminological vocabulary is already well suited to talk about crimes.

This paper has shown that the criminological vocabulary can account for the sociotechnical association of the rational criminal and the novel changes in the design of systems. Using a modest genealogical approach and starting from the ANT agnosticism principle, we have followed security engineers working on timesharing systems. They stated they were facing a new criminal situation: “a new wine”, the coupling of malicious users and timesharing requirements. Engineer-criminologists saw a mutual co-construction of the criminal and the computer-network environment where direct programming access via networked terminals created the conditions for malicious user to emerge. Engineer-criminologists of timesharing came up with a "new bottle" to contain the "new wine", composed of two elements. Firstly a perspective for which the solution to malicious users is not in formal controls (the Law) but in designing the (computer-network) environment; secondly a set of countermeasures selected depending on an analysis of possible risks/threats and based on a rationalisation of costs. We have then seen how engineers embraced a situational perspective largely similar to the criminological perspectives of SCP and RAT, while at the same time remaining symmetrical in talking about people and technologies.

To understand the relevance of this result and how this connects to theory, we can reconsider Latour's (1990) well-known example of the hotel manager who has the problem of convincing his clients to bring the key back to the reception. The clients are the deviant offenders, the hotel keys are the target and the manager is the not very capable guardian. In RAT studies, these three elements are given (i.e. the rational criminal, the VIVA aspects of the target) and it is the interplay among them which leads to the emergent property of a crime opportunity: the clients do not bring the key back because the guardian is not capable of securing the target, thus the formula O (clients) + T (keys) – G (manager) = Deviance. In Latour's example, however, at one point the manager introduces an innovation, which also is an Opportunity-Reducing Technique increasing the Inertia of the target: the addition of a metal weight, makes it uncomfortable for offenders to carry the keys around. The innovation restructures the entire situation and the roles: the guardian becomes capable, the key is much less a target and deviant clients become rule observers. What this paper has shown then is that the O+T-G=C formula can be used to understand the symmetries in the NoC. We need to consider that elements of the formula may translate due to innovations - the novelties we are looking to address - which lead to a wider reshape of the situation. Then, rather than seeing the situation only from the perspective of the offenders, we should look at how novelties (very often designed non-humans) restructure all the roles, including that of the offender. In other words, the O+T-G=C formula is a translation process. SCP, differently from RAT, operates with a slightly different approach as criminologists study the crime situation but then also make interventions with Opportunity-Reducing Techniques. To an extent they are the engineer-criminologists of terrestrial crimes. SCP has not been used much in cybercrime studies however, beyond some contributions related to how organisations deal with non-technical aspects of security, especially focusing on insider threats (Willison and Siponen, 2009). This limited use of SCP in cybercrime studies may be due to the considerations that security engineers occupy the situational crime prevention space in digital environments.

While a genealogical approach coupled with the agnosticism principle to the study of security may not have been the only way to reach the same results, the approach presents fundamental advantages. In addition to taking an open ended perspective on theory development, it has allowed us to reconsider ideas that nowadays are stable knowledge but that were far from obvious in the past. The first such idea is that programmers, including malicious ones, can directly program and even take control of a computer and that they can do so remotely using computer networks such as the Internet. Linking this to the current situation, Timesharing systems also contained the kernel of some contemporary applications where many users share a common pool of resources. Cloud computing is an example, where for instance Software as a Service (SaaS) is offered to a multitude of end-users (Nemani, 2011). Moreover, in some

Timesharing, security was initially overlooked or had to be retrofitted. This seems to be a situation which has presented itself again, for example with the Internet of Things, where many devices lack a number of security requirements (HPE, 2015).

Like most research this study also has some limitations. One aspect is certainly related with presenting a single case study. However, we should consider this work the first step toward bridging the NoC problem with a sociotechnical perspective and call for the conduction of further research. In my view, van der Wagen and Pieters (2015) also took a relevant step in this direction, but the limitation to their work is in using the standard ANT vocabulary, which does not facilitate broader dialogue with criminology and information security. Future directions for research will include testing the symmetrical treatment of the O+T-G=C translation formula in other case studies and contexts. An historical genealogical perspective may remain fundamental here, but approaching contemporary cases related with the Internet and novel arrangements of Information Technologies could also prove important.

References

Akrich, M., & Latour, B. (1992). A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. In W. Bijker & J. Law (Eds.) *Shaping technology, building society: studies in sociotechnical change* (pp. 259-264). Cambridge, MA: MIT Press.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Bayne, J. (2002). An overview of threat and risk assessment. *SANS Institute.* Retrieved from https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

Bijker, W. E., Hughes, T. P., Pinch, T., & Douglas, D. G. (2012). *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge MA: MIT press.

Bossler, A.M., & Holt, T.J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Callon, M. (1984). Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. *The Sociological Review*, *32*(S1), 196-233.

Callon, M. (1987). Society in the making: the study of technology as a tool for sociological analysis. In W. Bijker, T. Huges. and T. Pinch (Eds.) *The social construction of technological systems: New directions in the sociology and history of technology* (pp. 83-103). Cambridge MA: MIT Press.

Clarke, R.V. (1980). Situational Crime Prevention: Theory and Practice. *The British Journal of Criminology*, *20*(2), 136-147.

Clarke, R.V. (Ed.) (1997). *Situational crime prevention*. New York: Harrow and Heston.

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *44*, 588-608.

Felson, M., & Clarke, R.V. (1998). Opportunity makes the thief. *Police research series, paper*, *98*. Retrieved from http://www.popcenter.org/library/reading/PDFs/Thief.pdf

Foucault, M. (1972). *The archaeology of knowledge.* New York: Pantheon Books.

Foucault, M. (2000). Questions of Method. In *Power: Essential Works of Michel Foucault,Vol. 3*. (pp. 223-238). New York: The New Press.

Grabosky, P.N. (2001). Virtual criminality: old wine in new bottles?. *Social and Legal Studies*, *10*(2), 243-250.

HPE (2015). *HPE Fortify and the Internet of Things.* Retrieved from http://go.saas.hpe.com/fod/internet-of-things .

Holt, T.J. & Bossler, A.M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Holt, T.J., Bossler, A.M., & Seigfried-Spellar, K.C. (2015). *Cybercrime and digital forensics: An introduction*. London & New York: Routledge.

Latour, B. (1990). Technology is society made durable. *The Sociological Review*, *38*(1), 103-131.

Law, J. (2004). *After method: Mess in social science research*. London: Routledge.

Leukfeldt, E.R., and Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

McCarthy, J. (1983). *Reminiscences on the history of time sharing*. Retrieved from http://www-formal.stanford.edu/jmc/history/timesharing/timesharing.html

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. *Home Office Research report, 75.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

Nemani, R. (2011). The journey from computer time-sharing to cloud computing: A literature review. *International Journal of Computer Science & Engineering Technology*, *1*(6), 267-273.

Parikka, J. (2007). *Digital contagions: A media archaeology of computer viruses*. New York: Peter Lang.

Silberschatz, A., Galvin, P.B. & Gagne, G. (2004). *Operating system concepts* (6th Edition). John Wiley & Sons.

van der Wagen, W. & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Wall D (1999). *Cybercrimes: New wine, no bottles?*. In P. Davies, P. Francis & V. Jupp V (Eds.) *Invisible Crimes* (pp. 105-139). Palgrave Macmillan UK.

Wall, D. (2001). *Cybercrimes and the internet*. In D. Wall (Ed.) *Crime and the internet*. London: Routledge.

Willison, R. & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133-137.

Yar, M. (2005). The Novelty of ‘Cybercrime’ An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427.

Sources

Anderson, J. (1972). *Computer security technology planning study*. Air Force Elec. Syst. Div. Rep. ESD-TR-73-51.

Baran, P. (1965). Communications, computers and people. *Proceedings of the 1965 Fall joint Computer Conference*, Part 2, 45-49.

Bell, D.E. & LaPadula, L.J. (1973). *Secure computer systems: Mathematical foundations* (No. MTR-2547-VOL-1). MITRE CORP BEDFORD MA.

Browne, P.S. (1972). Computer security: a survey. *ACM Sigmis Database*, *4*(3), 1-12.

David, E.E. & Fano, R.M .(1965). Some thoughts about the social implications of accessible computing. *Proceedings of the November 30--December 1, 1965, fall joint computer conference, part I* (pp. 243-247). ACM.

Graham, R.M. (1968). Protection in an information processing utility. *Communications of the ACM, 11*(5), 365-369.

Graham, G.S. & Denning, P.J. (1972). Protection: principles and practice. In *Proceedings of the May 16-18, 1972, spring joint computer conference* (pp. 417-429). ACM.

Karger, P. A. & Schell R. R. (1974). *Multics Security Evaluation: Vulnerability Analysis*. Electronic Systems Division (AFSC), Hanscom AFB, Mass., ESD-TR-74-193, Vol. II, June 1974.

Lampson, B.W. (1969). Dynamic protection structures. In *Proceedings of the November 18-20, 1969, fall joint computer conference* (pp. 27-38). ACM.

Lampson, B.W. (1974). Protection. *ACM SIGOPS Operating Systems Review*, *8*(1), 18-24.

Parker, D.B. (1973a). *Manual for investigation of computer related incidents of intentionally caused losses, injuries, and damage.* Technical Report, California Univ., Livermore (USA). Lawrence Livermore Lab.

Parker, D.B. (1973b). *Threats to computer systems*. Technical Report, California Univ., Livermore (USA). Lawrence Livermore Lab.

Peters, B. (1967). Security considerations in a multi-programmed computer system. *Proceedings of the April 18-20, 1967, spring joint computer conference* (pp. 283-286). ACM.

Petersen, H.E. & Turn, R. (1967). System implications of information privacy. *Proceedings of the April 18-20, 1967, spring joint computer conference* (pp. 291-300). ACM.

Saltzer, J.H. & Schroeder, M.D. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278-1308.

Saltzer, J.H. (1974). Protection and the control of information sharing in Multics. *Communications of the ACM, 17*(7), 388-402.

Sorenson, J.L. (1972). Common Sense In Computer Security. *The CPA Journal*, *42*(5): 379-382.

Turn, R. & Petersen, H.E. (1970). *Security of computerized information systems* (No. RAND-P-4405). RAND Corporation Santa Monica California.

Van Tassel, D. (1970). Computer crime. *Proceedings of the November 17-19, 1970, fall joint computer conference* (pp. 445-450). ACM.

Ware, W.H. (1967a). Security and privacy: similarities and differences. *Proceedings of the April 18-20, 1967, spring joint computer conference* (pp. 287-290). ACM.

Ware, W.H. (1967b). Security and privacy in computer systems. *Proceedings of the April 18-20, 1967, spring joint computer conference* (pp. 279-282). ACM.

Weissman, C. (1969). Security controls in the ADEPT-50 time-sharing system. *Proceedings of the November 18-20, 1969, fall joint computer conference* (pp. 119-133). ACM.