Chapter 9
Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT)

Pompeu Casanovas

Abstract OSINT stands for *Open Source Intelligence*, (O)SI for (*Open*) *Social Intelligence*, and PbD for *Privacy by Design*. The CAPER EU project has built an OSINT solution oriented to the prevention of organized crime. How to balance freedom and security? This chapter describes a way to embed the legal and ethical issues raised by the General Data Reform Package (GDRP) in Europe into security and surveillance platforms. It focuses on the indirect strategy to flesh out ethical principles through Semantic Web Regulatory Models (SWRM), and discusses the possibility to extend them to Cyber Warfare. Institutional design and the possibility to build up a Meta-rule of law are also discussed.

Keywords OSINT • Social Intelligence • Privacy • Security • Semantic Web • Regulatory Models

9.1 Preliminaries: The Legal and Political Problem

There are many ways to conceptualise intelligence —individual, collective, swarm, etc. — to describe and research how it works or how to use it in courses of action. Since 2001, this practical side has received a strong boost. The explosion of Internet, the wide use of HTML protocols, and the speeding of the Semantic Web through W3C standards, is related to it (Casanovas et al. 2016a). But inaugurating the century with the *global terrorist threat* after September 11th was key to fund new research programs for military use. Some of these programs are focused on Open Source Intelligence (OSINT).

P. Casanovas (✉)
Institute of Law and Technology, Autonomous University of Barcelona, Barcelona, Spain

Faculty of Business and Law, Data to Decisions Cooperative Research Centre, Deakin University, Geelong, VIC, Australia
e-mail: pompeu.casanovas@uab.com; p.casanovasromeu@deakin.edu.au

M. Taddeo, L. Glorioso (eds.), *Ethics and Policies for Cyber Operations*,
Philosophical Studies Series 124, DOI 10.1007/978-3-319-45300-2_9

The word is somehow misleading, mostly due to the venerable history of Open Source (OS) in computing. There is also an ongoing discussion in legal theory on the role that OS plays in intellectual property, licenses, publishing and patents. Yet, when applied to intelligence, OSINT does not simply refer to the origin of the digital outcome, but to the legal and political sphere of the community where the "intelligent" outcome is encapsulated, distributed, reused and transformed.

What does it mean for a document, an image, a video to be qualified as OSINT? We could state that it basically means to place it in a public domain or, better, in *no man's land* domain, free to be grabbed and manipulated *for public reasons* —by LEAs (Law Enforcement Agencies), Intelligence Services, State Agencies… [1] But, as I will contend later on, many restrictions apply. There is no clear-cut line separating the *private* and *public* domains. Rather, there is a grey continuum zone bridging the two areas.

This chapter deals with the relationships and differences between (Open) Social Intelligence (OSI) and Open Source Intelligence (OSINT) or, in other words, with how to combine freedom and surveillance. This is currently one of the hot topics in European legislation and it is worthwhile to face it from a regulatory point of view.

The General Data Protection Reform package (GDPR) is at stake. European data protection law has been under review for a long time, eventually resulting in the recently approved General Data Protection Regulation (April 14th 2016).[2] The new rules intend to put citizens back in control of their data, notably through: (i) the right to be forgotten (when you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted); (ii) easier access to your own data (a right to data portability to make easier to transfer personal data between service providers); (iii) putting citizens in control (requirement of explicit consent to process personal data), (iv) Privacy by Design (PbD) and Privacy by Default (PbD) —as they are becoming essential principles in EU Data Protection Rules (EU Commission 2014).

The Opinion 28 released by the European Group on Ethics of 20 May 2014 described Ethics of Security and Surveillance Technologies (EGE 2014a). The Opinion advanced a set of sixteen concrete recommendations for the attention of the EU, member states, and a range of public and private stakeholders. It "*challenges the notion that 'security' and 'freedom' can be traded against one another*", and "*calls for a more nuanced approach, in which the proportionality and effectiveness of security and surveillance technologies are subject to rigorous assessment, and in which rights are prioritized rather than traded*". Certain core principles, such as human dignity, cannot be traded (EGE 2014b).

---

[1] This chapter is partially based on my work at the EU Network on Social Intelligence (SINTELNET) http://www.sintelnet.eu/. I revised some of my previous positions on OSINT (Casanovas 2014).

[2] Cfr. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) COM/2012/011 final – 2012/0011 (COD). After 4 years, the final draft of April 6th was finally approved by the EU Parliement on April 14th 2016. See http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf. For a useful and short summary of its content, see Albrecht (December, Albrecht 2015) and de Hert and Papakonstantinou (2016).

In the same vein, the EU Data Protection authorities and the Article 29 Working Party, on its plenary meeting of 25 November 2014, adopted a Declaration on European Values with 16 points (A29, 2014a).[3] Point one and two state that:

1. *The protection of personal data is a fundamental right. Personal data (which includes metadata) may not be treated solely as an object of trade, an economic asset or a common good.*
2. *Data protection rights must be balanced with other fundamental rights, including non-discrimination and freedom of expression, which are of equal value in a democratic society. They must also be balanced with the need for security.*

What does it exactly mean? Replacing the mechanism of security as a *general exception* to rules by another approach in which other principles apply adds some complexity to the balance between freedom and security.[4] The Common Law tradition (both British and American) is not considering protection of privacy as a fundamental right so far (Donohue 2005-06; Moshirnia 2013). Along with the upcoming Directive on personal data processing in criminal matters,[5] GDPR shapes a new general framework for the protection and exercise of rights. The final Regulation consists of 99 articles and 179 Recitals.[6]

I will contend that the epistemic approach to strike such a balance requires an additional level of analysis to figure out a general structure to compare the outcomes

[3] This Opinion must be completed with the WP29 Opinion on the legal grounds of surveillance of electronic communications for intelligence and national security purposes that was adopted on April 10th 2014. The origins of the statement are clearly expressed: "*The focus of this Opinion lies with the follow up that is needed after the Snowden revelations*." A major part of the Working Document discusses the applicability of the transfer regime of Directive 95/46/EC.

[4] Quoting Marju Lauristin (Raporteur) at the recent Debate on the protection of individuals with regard to the processing of personal data for the purposes of crime prevention (Strasbourg, Wednesday, 13 April 2016): "*In this framework, the very important thing is that the general principles of proportionality, legitimacy and purpose-limitation are included in police work. That means that no form of mass surveillance is possible. The collection of data is not possible. Retention for an unlimited or unclear period is not possible. Another important point is that we foresee the inclusion of data protection professionals in the police institutional setting: specifically, in police work*." http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20160413+ITEM-015+DOC+XML+V0//EN&language=en&query=INTERV&detail=3-515-000

[5] *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (05418/1/2016 – C8-0139/2016 – 2012/0010(COD))*{SEC(2012) 72 final}. See the text of the draft adopted on March 14th 2014 at the first reading at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2016-0126, and at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0219+0+DOC+PDF+V0//EN. It is now at the second reading now.

[6] Recital 19 states that GDPR does not apply to "*the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data*".

that I will call *Meta-rule of law*. This is also needed when addressing the issue of using OSINT not only to fight organised crime, but cyber-attacks and terrorism.

This chapter is divided into four sections. The first one draws a distinction between Open Source and Social Intelligence. The second one is centred on Privacy by Design polices. In Section 3 I introduce the CAPER regulatory model to facilitate the regulation of intelligence-driven policing platforms to fight organised crime.[7] Finally, I will defend, with some limitations, the extension of such a model to cyber warfare, advancing ten preliminary observations.

As a synthesis of my position: (i) even in surveillance toolkits and serious security issues some feasible ways to bridge PbD principles and citizens' rights are possible; (ii) PbD can be broadly understood as a form of institutional design; (iii) to balance security and freedom, to comply with existing regulations, and to foster trust, *intermediate regulatory models* based on hard law, policies, soft law (standards) and ethics are required; (iv) these models could also be used to solve some of the regulatory and legal puzzles raised by the *Tallinn Manual on the International Law applicable to Cyber Warfare* (2013).

9.2 Open Source Intelligence (OSINT) and Social Intelligence (OSI)

9.2.1 OSINT

OSINT has a military origin. Gathering knowledge from open source information lies on very practical reasons, not only on the development of data mining, big data and cloud computing. Mark Pythian (2009) observes that collection techniques that worked well in a Cold War context are not that useful in the end of the twentieth century. Recruiting agents within Al-Qaeda, or attempting to infiltrate Islamic radical groups is a nearly impossible task for Western agencies.[8]

Our technological approach should acknowledge that the process to gather publically available information is not new either. Web 2.0 and 3.0 are just *enhancing* the heuristic behaviour of producing knowledge through all possible sources. For instance, libraries have always been a source of information to turn it into usable knowledge after intensive queries. Now, they have emerged again on the international scene as a critical source of soft power (McCary 2013).

---

[7] *Collaborative Information, Acquisition, Processing and Reporting for the Prevention of Organized Crime* (CAPER) http://www.fp7-caper.eu/

[8] Phythian (2009: 68–69) graphically quotes a former CIA operative about this, down to earth:

> The CIA probably doesn't have a single truly qualified Arabic-speaking officer of Middle Eastern background who can play a believable Muslim fundamentalist who would volunteer to spend years of his life with shitty food and no women in the mountains of Afghanistan. For Christ's sake, most case officers live in the suburbs of Virginia. We don't do that kind of thing.

There is no homogeneous definition of the term OSINT. It depends on the field, purposes and actions in which it is used. Within the intelligence community, OSINT is usually defined as unclassified information obtained from any publicly available source in print, electronic, or verbal form (radio, television, newspapers, journals, internet, commercial databases, and video). The process to gather intelligence in this way begins with raw information from primary sources assembled through filtering and editing processes. OSINT is then "constructed". Only after the process has been completed, OSINT is created (Burke 2007).

Intelligence Services refer to OSINT according to military uses as "unclassified information that has been deliberately discovered (…) to a select audience" (Steele 2007).[9] Not all collections and accesses to information sources fall equally under this definition. Several requirements should be satisfied as preliminary conditions (Jardines 2015). The information must be: (i) publicly available, (ii) lawful, (iii) properly vetted, (iv) acquired second hand, (v) and be produced to satisfy an intelligence requirement. In this sense, it has been already incorporated into the context of US Military as a new useful analytical dimension in addition to human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signatures intelligence (MASINT).

The NATO early published in 2001 and 2002 three OSINT Handbooks, now accessible online: the *NATO Open Source Intelligence Reader*, the *NATO OSINT Reader*, and the *Intelligence Exploitation of the Internet.*

Reports for the US Congress are quite clear about its wide adoption: "A consensus now exists that OSINT must be systematically collected and should constitute an essential component of analytical products" (Best and Cummings 2008).

9.2.2 (Open) Social Intelligence (OSI)

OSINT is considered also for other non-military purposes as a cluster of tools to browse the web, aggregate information, and getting reliable profiles from websites, blogs, social networks, and other public digital spaces. From this broader point of view, it may be defined synthetically as "the retrieval, extraction and analysis of information from publicly available sources" (Best 2008), without further requirements. This approach is taken by many to get, structure and manage information in a broad array of social domains —e.g. media (Bradbury 2011), education (Kim et al. 2013), business (Fleisher 2008), disaster management (Backfried et al. 2012), and fire services (Robson 2009). It entails a definition of the concept referring to

[9] This is the official definition (*US Army FM 2-0 Intelligence March 2010*), based on National Defence Autorization Act for FY 2006, & 931: 1. *Open-source intelligence is the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. Open-source intelligence (OSINT) is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements.*

functions being performed by a computer system —retrieval, extraction and analysis of information. Thus, it is ostensive in nature, offering a descriptive meaning.

It is worth to notice that OSINT consists of reusable and reused (second hand) information, embedded into broader courses of action, with a display of possible frameworks and changing scenarios. The difference between military and non-military uses lies on the type of frameworks, stakeholders, players, and organisations involved in sharing and reusing data and metadata, rather than on the information content. Two more features matter: the type of technology used, and the direction of the workflow in the communication framework (top down or bottom up).

Mobile technologies are usually linked to crowdsourced usages of content (Poblet 2011). Crowdsourced platforms, micro-tasking, crisis mapping, and cooperative organisations face OSINT from a *cooperative* and a *collective* point of view, empowering people to obtain a common end (Poblet et al. 2014). Large amounts of data can be gathered, analysed and conveyed online and in near real time.

This is not incompatible with police or military functions, as long as they monitor crowd participation. E.g. in the London and Vancouver riots of 2011, Legal Enforcement Agents (LEAs) obtained such voluntary cooperation (Keane and Bell 2013).

Let's follow this thread. *Collective* or *Social Intelligence* are scientific terms, developed by research communities in Artificial Intelligence, Cognitive Science and Social and Political Sciences.[10] OSINT is a rather functional, pragmatic term used when collecting open source information for some specific purposes. Could OSINT be related to (Open) Social Intelligence (OSI)?

Both concepts —OSI and OSINT— have an operational side and denote the circulation and transformation of non-structured information into structured information on the Web. In their history of the concept, Glassman and Klang (2012) offer a communicative and cultural approach —"the Web as an extension of mind", OSINT as the interface between *fluid intelligence* and *crystallized intelligence* (Backfried et al. 2012).

If this is so, the field, methodology and theory of Social Intelligence could comprehend what is referred by OSINT, as the social mind is faced as a set of social affordances that can be represented, described and reproduced computationally as *inner* mechanisms, as social *artefacts* performing a collective work (Castelfranchi 2014). Social Intelligence focuses on the human/machine coordination of *artificial socio-cognitive technical systems*, assuming that they interact in a shared web-mediated space with aims, purposes, intentions, etc. and are amenable to models *and* meta-models from a theoretical point of view (Noriega et al. 2014).

If the concept of OSINT is used to describe the operational functionalities of a computational system, this use could be embedded into a conceptually broader set of notions to be effective. In artificial socio-cognitive systems "rationality is based on the model that agents have of the other agents in the system" (Noriega and d'Iverno 2014). This epistemic assumption is not necessary for OSINT systems,

[10] Cfr. http://www.sintelnet.eu/

more pragmatically oriented and centred on visual analytics and on the interface between intra and inter-organizational teams.

I will only address the political side of the problem, as governance and the issues related to international and humanitarian law are crucial. Which meta-model would be needed to build *at the same time* military and police uses, and the institutional design of privacy and civil rights protections (striking a balance between freedom and security)? This is certainly a challenge, for which I will make use of a socio-cognitive perspective based on open social intelligence (OSI).

9.3 The CAPER strategy

9.3.1 Intelligence-Led Policing and the Law

Organised crime is a difficult subject of study. Authors have found that priority setting and strategic planning in the field of organised crime is inherently characterized by uncertainty (Verfaille and Beken 2008). The big numbers of illegal activities and cybercrime in particular, are hard to assess accurately. In this new field, "the global nature of the cybercrime industry inherently downplays the role of localized law-enforcement agencies" (Kshetri 2010, 247).

To fight it, from some time now, European LEAs have adopted intelligence-led policing as a method: "*the application of criminal intelligence analysis in order to facilitate crime reduction and prevention in a criminal environment through effective policing strategies and external partnership projects"* (Ratcliffe 2003, 2008). O'Connnor (2006) adds to this definition the use of intelligence products for decision-making both at the tactical and strategic level. Strategic intelligence refers to pattern and trend analysis of crime indicators, as opposed to tactical intelligence, which is anything evidential or helpful in making a case. There are four primary types of analytic outcomes provided by an intelligence-led police department on individual or group behaviour: (i) profiles, (ii) briefs (fact patterns related to investigative hypothesis), (iii) assessments, (iv) estimates (forecast or predictive statements) (O'Connor 2006).

OSINT is not limited to police departments. Specialized companies, attentive to geopolitical indicators, leverage OSINT and combine it with big data analytics. Zeeshan-Ul-Hassan Usmani (2014) underlines the point of terrorist predictions:

> *We need to focus more on the OSINT, the 'open-source intelligence' databases, the things that we can gather from online blogs, online magazines-for example, if we can see the way they recruit. We can get quite a few hints here and there from the online blogs and chat rooms. So we need to account for that. Second, technically you need to account for the geopolitical indicators, defined as GPIs. […] Here is another bizarre example: Pakistan and India are natural rivals when it comes to cricket matches. Both teams had played 18 one-day matches since 2007. India won ten and nothing happened, Pakistan won eight and the probability of getting a terrorist attack within 24 h of winning against India is 100 %. Correlation doesn't mean causation, so there might be other factors in play. For example, when Pakistan wins we have thousands of people on street dancing, which makes them an*

easy target. Perhaps separatist groups do not like the nation to be happy about anything or some other reason, but we know we have this probability and we can use it for better protection and warnings.

Social media data renders social life more visible to police and other investigators (Trottier 2014). When it comes to security and surveillance issues, national and transnational differences are notable. In Europe, principles such as consent, subject access, and accountability are core to current legislation and to the General Data Protection Reform package (GDRP). The individual is deemed to keep control over the personal data being collected. Informational rights are usually known as the ARCO rights (access, rectification, cancellation, and objection). LEAs' behaviour must be compliant with regional, national, and EU laws.

The problem of dealing with law is that *law* is not a well-defined field. Rules, norms, principles and values are expressed in natural language, and there is a real problem to address them analytically, for the same statute, article, principle or concept might be *interpreted* in different ways whenever instantiated in a decision or a ruling (Casanovas 2014).

Technically, this can be faced as an "interoperability" problem, except for the fact that law always resists complete modelling, as shown by the integration of domain and core ontologies into upper-level ones (Casellas et al. 2005), and the interactive dimension of ontology-building (Casanovas et al. 2007). Consequently, since there are objective limitations to formalise legal statements, the analyst is forced to complete this missing part by settling some general framework by her own.

Practical decisions and implementation of norms are usually ground in some theory. From an epistemic point of view, the analyst is simultaneously working with an operational language and the structuring meta-system for such a language. Models and meta-models come together, and one of the most interesting tasks is to reveal the inner structure of the framework (the meta-model) of legal interpretations.

CAPER is an OSINT platform to fight organised crime and to facilitate transnational cooperation (Aliprandi et al. 2014). The meta-model for CAPER has been detailed in eight Deliverables and some articles and papers (Casanovas et al. 2014a, b; González-Conejero et al. 2014; Casanovas 2014, 2015a, b). In the CAPER workflow, privacy by design policies and ethical guidelines to protect citizens' rights have been worked out simultaneously to build a CAPER platform compliant with legal and ethical specifications.

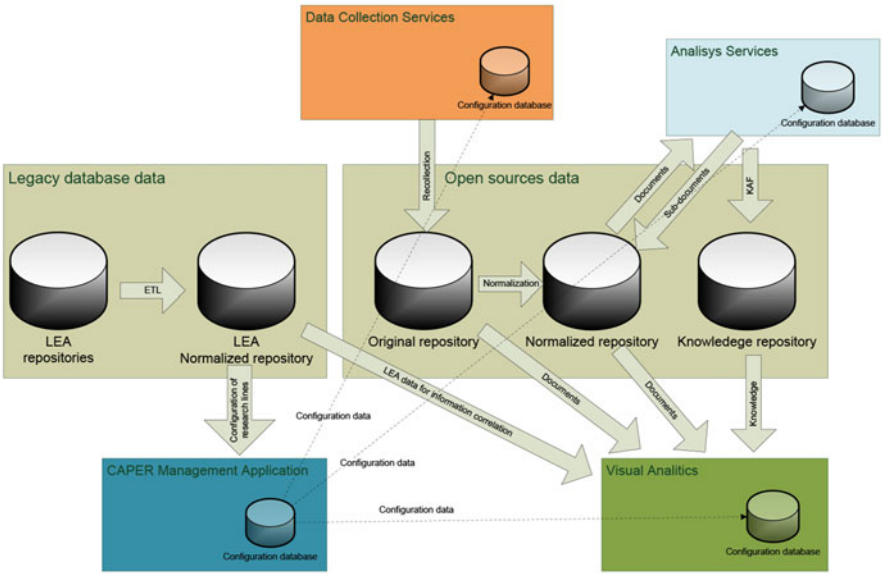

Fig. 9.1 CAPER databases overview. Source: http://www.fp7-caper.eu/results.html

9.3.2 The CAPER Workflow

The functionalities of the CAPER platform are manifold[11]: (i) implementing a framework to perform the task of connecting multiple data sources with multiple visualization techniques via a standardized data interface, including support for data-mining components; (ii) enabling a quick import of data types from disparate data sources in order to improve the ability of different LEAs to work collaboratively; (iii) supporting pattern discovery, documentation and reuse, thus increasing progressively detection capabilities. The architecture design has four components: (i) data harvesting (knowledge acquisition: data gathering), (ii) analysis (content processing), (iii) semantic storage and retrieval, (iv) and advanced visualization and visual analytics of data. Figure 9.1 below shows the interaction and workflow between databases.

Besides a specific Privacy Impact Assessment (PIA), we explored several related strategies that constitute an *indirect* approach to PbD principles (Casanovas et al. 2014a, b). This is the final result:

1. The CAPER workflow is addressed to four different LEA's analysts: (i) The *Generic Analyst* (GA) (ii) the *Advanced Analyst* (LEA-AA) (iii) the *System Administrator*, (iv) LEA's External User (LEU).

[11] Most Deliverables were confidential. I am offering here a standard synthetic description, as in Casanovas et al. (2014b).

2. Well-defined scenarios are extracted from the experience of managing specific types of crimes. CAPER tools operate only within the investigation conducted by LEAs, helping them to better define the lines of research, but avoiding any automated conceptualisation of them.
3. Well-defined module interdependencies are drawn in advance. The CAPER crawling system is sustained by three modules: (i) crawler by keyboard, (ii) by URL, (iii) by URL focusing on keyboards. The crawler is also able to convert images and videos metadata into allowed mimetypes required by the *Visual Analytics* module (VA). Multi-lingual semantics is added to the whole process as well.
4. Two different ontologies have been built: (i) a Multi-lingual Crime Ontology (MCO) for 13 languages, including Hebrew and Arabic, with a proof of concept on drugs (346 nodes). MCO adjusts to country legislations (e.g. possession of drugs is a crime in UK, but not in Spain); (ii) a legal ontology focusing on European LEAs Interoperability (ELIO). ELIO has been built with the aim to improve the acquisition and sharing of information between European LEAs (González-Conejero et al. 2014).

9.3.3 PbD and Security

The concepts of Privacy by Design (PbD) —and Data Protection by Design and by Default— are well known in the computer science and legal research communities (Cavoukian 2010). This conceptual body aims at developing the Principles of Fair Information Practices (FIPs)[12] that follow from the Alan Westin tradition in private law,[13] and the technological idea of a meta-layer to manage and secure the identity of users on the web set by the Microsoft architect Kim Cameron (2005).

Ann Cavoukian (2012) asserts that "*it is not true that privacy and security are mutually opposing"*, and that big and smart data "*proactively builds privacy and security in"*. It might be true, but it is not evident in the fight against organised crime. Both in the military and humanitarian fields, to be effective OSINT tools have been designed just for what they should be controlled: spotting as much as possible and getting personal information about individuals and organizations.

Bert-Jaap Koops, Jaap-Henk Hoepman and Ronald Leenes (2013, 2014) experienced this void on the sidelines of law and technology when they faced the problem of modelling the protections of General Data Reform Package into OSINT platforms.[14] As might be expected, they found that privacy regulations cannot be hardcoded —"*'privacy by design' should not be interpreted as trying to achieve rule*

[12] 1. Openess and Transparency, 2. Individual Participation. 3. Collection Limitation, 4. Data Quality, 5. Use Limitation, 6. Reasonable Security. 7. Accountability.

[13] These historical origins must still be retraced and reconstructed carefully. I am grateful to Graham Greenleaf for this observation.

[14] VIRTUOSO (*Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitations)*, http://www.virtuoso.eu/.

compliance by techno-regulation. Instead, fostering the right mindset of those responsible for developing and running data processing systems may prove to be more productive. Therefore, in terms of the regulatory tool-box, privacy by design should be approached less from a 'code' perspective, but rather from the perspective of 'communication' strategies [emphasis added]". Quite recently, the concept of "tactics" has been introduced by Colesky et al. (2016) to bridge the gap between legal data protection requirements and system development practice.

I subscribe the authors' guidelines, but perhaps another conclusion could be drawn from these limitations. There are other possibilities to embed PbD into surveillance platforms, albeit indirectly, i.e. adding theoretical views not thinking of *techno-regulation* nor *communication* but of what law means when constructed through technological means. It is the field of *intermediate institutional models* what might be worked out from the perspective of self-governance and socio-cognitive artificial systems.

9.3.4 PbD Strategies and CAPER Rules

Design also means *institutional design*. The notion of *institutional-Semantic Web Regulatory Model* (i-SWRM) leans on this assumption: a self-regulatory model embeds the dimension of PbD into a technological environment than can be represented as a social ecosystem (Casanovas 2015a, see below Sect. 9.4.2). In some domains —licensing, patents, or intellectual property rights— such an ecosystem entails an automated link between normative compliance and the effective legal action that implements some rights (Rodriguez-Doncel et al. 2016). OSINT platforms for massive surveillance require a different strategy. With some differences, the CAPER ecosystem is similar to the framework set by Koops et al. (2013) and specifically by Hoepman (2014).

Hoepman's PbD strategies model focuses on the inner structure of the modelling; signalling several points into a general framework for privacy (or data protection) closed managerial system. This is consistent with the idea of concentrating the effort on the interpretation of the law, leaving aside the specific problems, risk scenarios, and asymmetric multilayered governance of OSINT platforms, end-users and LEAs. Conversely, i-SWRMs and specifically the regulatory model designed to regulate the CAPER workflow system (CRM), are more focused on LEA's inner and outer relationships. The social ecosystem centred on the specific data that users are processing and "living by" can be outlined as a simple scheme described in advance (see Fig. 9.2).

To implement the rules contained in the CAPER final recommendations as guidelines to run and monitor the platform, we might place first the potential risks on its information flow (Fig. 9.3).[15] E.g. a rule like "The storage of the CAPER data should be implemented in a separate repository. No contact with ordinary criminal

[15] A Private Impact Assessment (PIA) was carried out all along the Project with LEA's analysts. Antoni Roig set the risks and rules in some non-public Deliverables (D7.2, D73. D7.5, and D7.6) and J. González-Conejero plotted them on the information workflow (Fig. 9.2). The CAPER Ethical Committee was composed by Ugo Pagallo, Giovanni Sartor, Danièle Bourcier, John Zeleznikow, and Josep Monserrat.

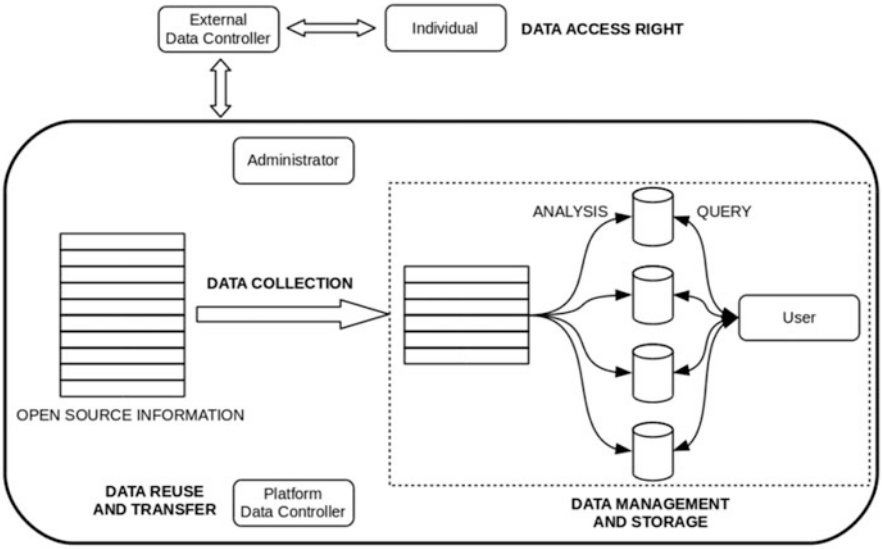

Fig. 9.2 CAPER regulatory scheme. Source: CAPER D7.8 (González-Conejero et al. 2014; Casanovas et al. 2014a, 2014b).

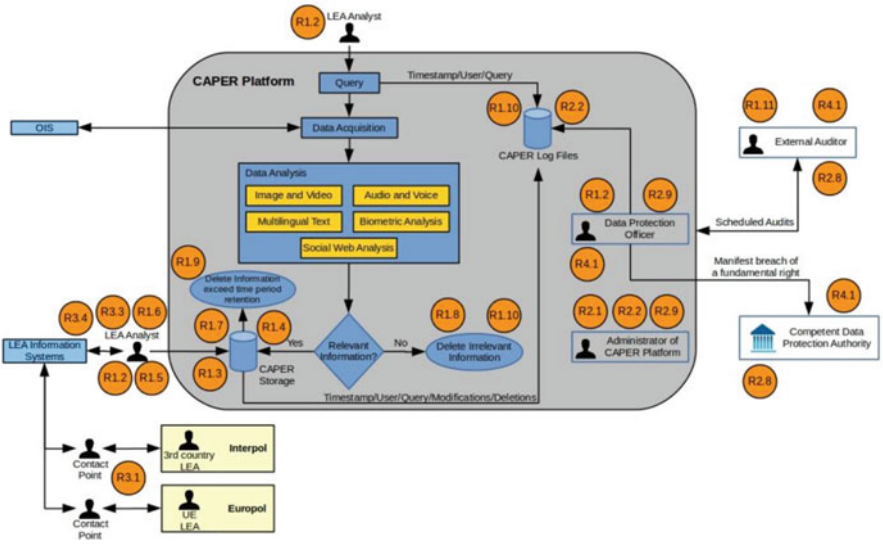

Fig. 9.3 Situated risks and rules onto the CAPER information workflow. Source: D7.6, D7.7. D7.8 CAPER (González-Conejero et al. 2014; Casanovas et al. 2014a, 2014b, http://www.fp7-caper.eu/results.html)

Table 9.1 Rules to regulate LEA's internal behaviour

I data collection and storage	R1.1 Each LEA should perform a specific Privacy Impact Assessment (PIA) according to the general framework offered by the CAPER Regulatory Model (CRM).
	R1.4 No automated classification of suspects, victims and witnesses can be inferred from CAPER results.
II Data management	R.2.3 Access to CAPER database should be granted for the purpose of prevention, detection or investigation of organized crime.
	R.2.4 Any other request of access for other purposes should be rejected.
	R.2.5 Non-authorised LEA and intelligence services or administrative bodies of authorized LEA should not have access to CAPER data.
	R.2.6 The use of system integrity tools should enable detection and reporting of changes applied on servers. In case of such an event the system should be able to notify specific users such as the creator of the query which results have been modified.
	R.2.7 Regular audits of the CAPER system should be performed by the external supervisor. The competent authority should be informed of the results, if necessary, according to national legislation, including the plans for enforcing recommendations.
III. Data reuse and transfer	R.3.2 No automated classification of suspects, victims and witnesses can be inferred from CAPER results.
IV Right of data access	R.4.2 The reasons to deny access should be clear and defined. Access can be denied when the access may jeopardise the fulfilment of the LEA tasks, or the rights and freedoms of third parties.
	R.4.2 The alleged reasons to deny access should be open to external supervision. The external supervisory authority should have free access to documents justifying the refusal. A short time-span of 3 months to give an answer to a previous request of access should be implemented.

Source: D7.8 Caper
Casanovas et al. (2014a, 2014b), http://www.fp7-caper.eu/results.html

data bases should be allowed" can be situated between the LEA analyst and repositories of raw data.

However, rules for the prevention of unauthorized access, data reuse and transfer, and for the protection of citizens' rights — e.g. the right to be notified when they notice that their personal data is being processed — cannot be plotted on the chart because they do not address solely the regulation of the information flow, but rights and obligations for citizens, third parties, controllers, and administrators. Regulations have a wider scope, covering functions, rules and players alike.

As stated, 9 out of the 23 designed rules cannot be situated because they don't apply to information processing, but to end-users' behaviour. R1.1, R1.4, R2.3, R2.4, R2.5, R2.6, R2.7, R3.2, R4.2, R4.3 are not plotted (Table 9.1). Under the new General Data Reform Package (GDRP) the scope of regulations is much wider. Thus, it is a hybrid model: some rules apply to the information processing flow, while others apply to the way how this information should be used, treated, protected and eventually deleted by analysts and internal controllers. This holds, e.g.

for a positive obligation such as "Each LEA should perform a specific Privacy Impact Assessment (PIA) according to the general framework offered by the CAPER Regulatory Model (CRM)", a general prohibition as "No automated classification of suspects, victims and witnesses can be inferred from CAPER results", and for specific obligations such as "The alleged reasons to deny access should be open to external supervision. The external supervisory authority should have free access to documents justifying the refusal. A short time-span of 3 months to give an answer to a previous request of access should be implemented".

9.4 The Regulation of OSINT Platforms

9.4.1 Rule and Meta-Rule of Law

What is the relationship between all these non-discrete categories? OSINT platforms raise a governance problem, because they should be as effective as possible to fulfil their goal to collect and store information, and at the same time they must comply with OSINT requirements, such as law compliance. Yet, organised crime has a transnational, extended dimension. There are about 3.600 organised crime organisations operating across Europe, with global connections. Therefore, what does "law compliance" mean?

Security, data, and privacy are the subject of quite different national regulations. Platforms and tools must respect statutes and regulations at the national level, attend the National and European Data Protection Agencies requirements, observe Human Rights case laws, and take into account LEA's professional best practices and culture. The notion of a *transnational rule of law* could be a good global strategy, since it grasps in a single concept all the legal sources while focusing on rights and regulations.

The rule of law implies that government officials and citizens are bound by and generally abide by the law, and legal pluralism refers to a context in which multiple legal forms coexist (Tamanaha 2011). Would it be possible to conceptualise and organise the relationship between rulers and ruled so that rulers themselves are subject to a rule of law in digital contexts, respecting pluralism?

In the absence of a transnational state, the notion of *Meta-level rule of law* has been coined at Elinor Ostrom's school to point to the tension between the "threat of chaos" and the "threat of tyranny" in the management of common perishable goods, such as water, wood or fisheries (Ostrom 2010; Aldrich 2010, Aligica and Boettke 2011). The "just right" solution lies in between. Rule of law scholars, such as Murkens (2007) and Palombella (2009, 2010) have recently pointed out the recoverable features of the classical model for transnational purposes as well (not bound by nation-state perspectives).

Michael Ritsch (2009) advances a "Virtual rule of law" for cyberspace. According to him, the "rule by law" [his spelling] must be: (1) non-arbitrary, (2) stable, (3)

public, (4) non-discretionary, (5) comprehensible, (6) prospective, (7) attainable, (8) consistently enforced, (9) impartially applied, and (10) adjudicated in a factually neutral way. "*These indicia, however, do not include traditional elements of "liberal" rule of law, including democracy and personal rights"* (Risch 2009, 2).

Jonathan Zittrain's idea of "generative" Internet is relevant here. Zittrain's seeks to maintain the Internet use community-based, into the users' hands.[16] Following Zittrain (2008) and Lessig (2006), Mark Burdon (2010) provides examples of the importance of standards from a law and technology perspective. He distinguishes between first generation privacy laws, based on the application of information principles to interactions, and Web 2.0 second generation laws, which should take into account the collective and aggregated dimension of crowdsourcing and public intervention. E.g. Privacy invasive geo-mashups are unavoidable with the use of Google-maps. The same situation is produced with the shared content needed in crisis mapping and the generalized use of local and personal images in disaster management (Poblet 2013). But potential solutions for the prevention and mitigation of privacy problems reside in the development of embedded technical and social standards, and not solely through "avenues of legal recourse founded on the concept of information privacy" (Burdon 2010, 50).

It is my contention that this problem should be tackled at different levels of abstraction: (i) the regulation-sourcing problem, in which the selection of legal sources is at play, should be treated both at the technical and regulatory dimension of the specific tool; (ii) the social regulatory ecosystem model set by Web Services and platforms (involving rights holders, managers and end-users); (iii) the conceptual meta-model drawn to design the regulatory system.

I will call *Meta-rule of law* the analytical management of rights and norms of the rule of law through computational models, information processing, and both virtual and physical organisations (Casanovas 2015a, 2015b). The CAPER Regulatory Model (CRM) is an example of this multi-layered and multi-dimensional approach.

9.4.2 CAPER Regulatory Model (CRM)

Figure 9.4 shows the emergence of institutional strengthening and trust from the two axes of the rule of law —binding power and social dialogue. The meta-model assumes that the degree of strength (*Macht*, *force*) exerted and the degree of non-cooperative behaviour is inversely proportional to the degree of dialogue and cooperation between rulers and ruled. In this way, the construction of a public space

[16] "The deciding factor in whether our current infrastructure can endure will be the sum of the perceptions and actions of its users. There are roles for traditional state sovereigns, pan-state organizations, and formal multistakeholder regimes to play. They can help reinforce the conditions necessary for generative blossoming, and they can also step in—with all the confusion and difficulty that notoriously attends regulation of a generative space—when mere generosity of spirit among people of goodwill cannot resolve conflict. But such generosity of spirit is a society's powerful first line of moderation." (Zittrain 2008, 246)

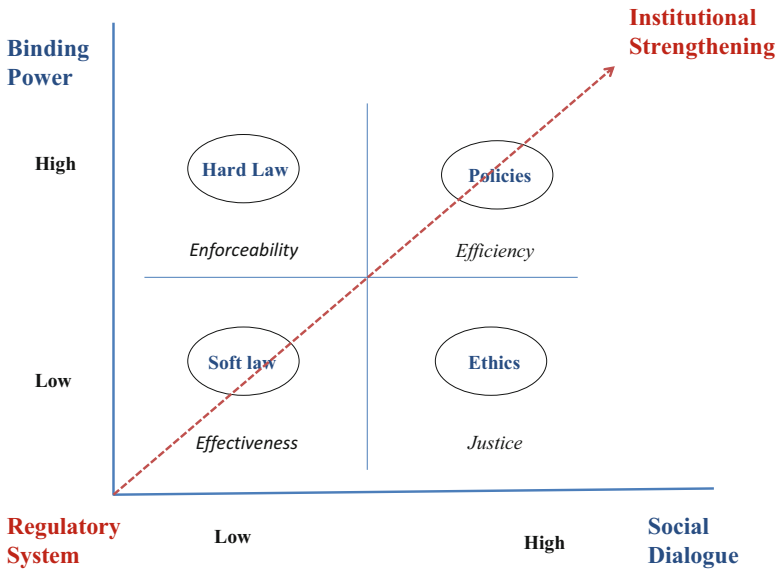

Fig. 9.4 CRM: Institutional strengthening *continuum*

depends on the combination of the regulatory components that can be ordered along the two axes to set up *intermediate institutions* such as the CAPER framework guidelines. This kind of institutions can be built to select legal sources and make them compatible with specific governance models.

Another way to describe them, drawing from classical legal theory, is to consider law application and implementation as the initial, framing point to instantiate the content of legal norms. Selection and interpretation of legal sources is a top-down semantic process (from some authorised bodies) as well as a pragmatic and dialectic one (stemming from the interaction of stakeholders, companies, citizens, consumers).

Figure 9.5 represents CRM dynamics. *Institutional strengthening* constitutes the third dimension emerging from the relationship between binding power and social dialogue, setting the regulatory system and fostering *trust*. Therefore, trust is a non-direct result coming out from a multilayered governance dynamics involving: (i) Courts (hard law), (ii) Agencies (policies), (iii) Experts (soft law), (iv) and Ethics (Committees balancing values, principles, and norms). It holds as a conceptual meta-model, framing the specific rules laid down for CAPER monitoring and managing. Enforceability, efficiency, effectiveness, and justice are first order properties, directly qualifying their space. *Validity* (of norms or rules) is a *second* order property, triggering *legality* — the final qualificatory stage of a behaviour, action or system. For a regulatory system be qualified as *legal* (or compliant with legality) it must be valid first, i.e. it must reach some threshold of compliance with first order properties. Both first and second order proprieties can be understood as graduated scales in a regulatory space. They are non-discrete categories (Casanovas 2013, Ciambra and Casanovas 2014).

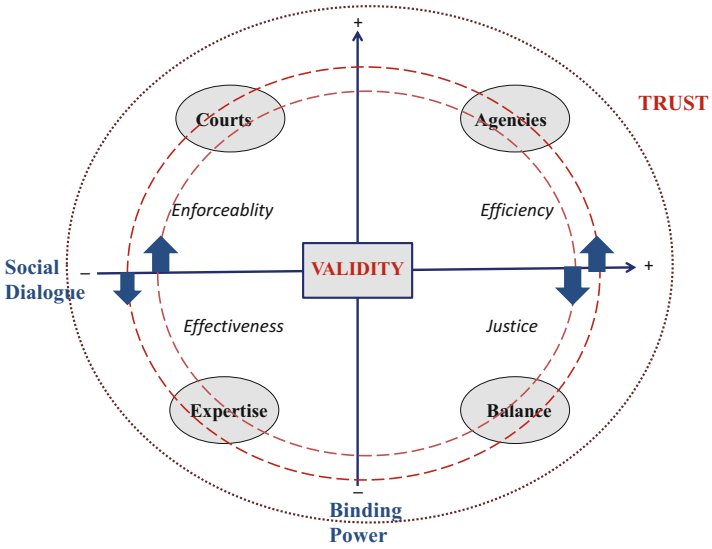

Fig. 9.5 CRM: Validity and trust dynamics

9.4.3 Normative and Institutional Semantic Web Regulatory Models

Semantic Web Regulatory Models (SWRM) co-organise the conceptual architecture of (enforceable) hard law and policies, and (non-enforceable) soft law, and ethics (Casanovas 2015a). They operate at the *in-between* space (digital/real) described by Floridi. In this hybrid, augmented, semantically enriched reality, formal compliance with norms should not be limited to their content, but it should be expanded to the sustainable endurance and maintenance of their effects too. Thus, the validity of the intermediate system is shown through the emerging independent axis of *institutional strengthening*. This approach presents the additional advantage of being measurable.

I distinguish between *Institutional-SWRM* and *Normative-SWRM*, according to the focus and degree of automated execution. Again, this distinction is not absolute. Any regulatory model set for a specific ecosystem contains elements of both. *Normative-SWRMs* make use of RDF, RuleML, and computer versions of rights, duties and obligations. They may lean on the use and reuse of nested ontologies or ontology design patterns (ODP), and *Rights Expression Languages* (REL) representing legal licenses, intellectual property rights, or patents as data and metadata to be searched, tracked or managed. Rights Expression Languages (REL) are based on the instantiation of rules that can be semantically populated by means of extended vocabularies to express policies.[17] Therefore, *end-users and systems are linked*

[17] Cfr. https://www.w3.org/community/odrl/

through the same tool that is being used to manage and apply the modelled policy and legal knowledge.

Institutional-SWRM (i-SWRM) are focused on the relationship of end-users with their self-organised system. Inner coordination among electronic agents, outer interface with human (collective) agents, and their dynamic interaction within different types of scenarios and real settings are crucial. They can be applied to regulatory systems with multiple normative sources and human-machine interactions between organizations, companies and administrations. Thus, their conceptual scheme is linked with legal pluralism and with existing models of asymmetric multi-layered and networked governance. These are conceptual constructs compatible with Elinor Ostrom's social philosophy —polycentricism and social ecosystems— because their centre of gravity lies on their dynamic social bonds. *End-users and systems are connected through the social and legal bonds that externally link them through intermediate legal and governance institutions*.

In the CAPER example, dialogue with LEAs and security experts constitute a key point to understand where do the problems lie and why, and to let LEA's investigators participate into the regulatory process. At the same time, control is exerted because binding norms apply as well. E.g. the need for an internal and external DP controller (competent DP authorities) and the obligation to set a strict log file to keep records to sustain the accountability of the whole system.

So, the Caper Regulatory Model (CRM) lying behind the actions taken intends to bridge negotiations of social agents with the normative requirements and conditions of the rule of law (reinterpreted from this broader standpoint). This is why it can be implemented among LEA's organizations and embedded into the CAPER system to regulate the use of the platform. CRM is an example of i-SWRM (even if there are few nested automated rules into the system architecture).

9.5 Could CRM Be Applied to Cyberwarfare?

9.5.1 Cyberwarfare

The CRM is a regulatory programme that has been designed to furnish a solution to the OSINT regulatory puzzle. It remains still unclear whether it can be applied with success to related subjects. This chapter constitutes a first step in this direction. I have outlined (i) a specific model, (ii) a more general meta-model to be applied to the OSINT landscape, and (iii) some new concepts for institutional design around the notions of regulatory systems, i-SWRM and n-SWRM. Especially the notion of Meta-rule of law is deemed to be used in a wider political context.

Surveillance over the civil population, a rational response to cyber-attacks, and protections against terrorist threats constitute different objectives and entail different tasks that should be coordinated, albeit they can be analysed separately and regulated differently.

It could be taken into account that, a bit surprisingly, the fight against organised crime is a much more precise topic than cyberwarfare. Experts have already stressed that cyberwarfare constitutes a field in which conventional regulatory tools for warfare have to be carefully restructured to solve "the 3 R problems": rights, risks and responsibilities (Taddeo 2012). Broadly speaking, in addition to land, sea, air and space, information sets a 5th dimension of warfare. A transversal, not always violent domain, but with a great potentiality to cause harm to specific targets; be the target a state, a high-tech company, a conventional corporation, or a political community (Orend 2014). Floridi and Taddeo (2014) have turned this dimension into *Information Warfare*.

There is no general agreement yet about how this new space should be monitored and regulated. The *Tallinn Manual on International Law applied to Cyber Warfare*, issued by distinguished scholars in the field and edited by M. N. Schmitt (2013), does not address the subject directly. OSINT is never specifically mentioned. It would be possible to connect it to related notions such as "Active Cyber Defence" or "Supervisory Control and Data Acquisition", but regulatory models are still viewed as state devices, and customary public international law as an inter-state affair (Schmitt and Watts 2014).[18] This approach is not to be thrown. From a legal perspective, it constitutes a realistic standpoint to deal with. Many experts are still working under this umbrella, endorsing a legal understanding that defines *cyber-attack* as "a trans-border cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects" (*Tallinn Manual*, Rule 30). Therefore, "cyberattacks are deemed to be simply another strategy or tactic of warfare, like armed drones and artillery barrages" (Solis 2014, 5).

Kilovaty (2014) distinguishes three conceptual perspectives: (i) Instrument-based approach, (ii) Target-based approach, (iii) Effects-based approach. He summarises the unsolved problems in the Tallinn definition: who would qualify as a combatant in the cyber context, what measures an attacked state can employ to repel a cyber-attack, and how the international law normally treats cyber espionage and the theft of intellectual property. As highlighted by Zeadally and Flowers (2014,15), the *Manual* definition of cyberwarfare excludes several relevant issues, e.g. cyber-operations designed to destabilize a nation-state's financial system since the attack does not directly result in death or physical destruction.

[18] *(…) as cyber activities become ever more central to the functioning of modern societies, the law is likely to adapt by affording them greater protection. It will impose obligations on states to act as responsible inhabitants of cyberspace, lower the point at which cyber operations violate the prohibition on the use of force, allow states to respond forcefully to some nondestructive cyber operations, and enhance the protection of cyber infrastructure, data, and activities during armed conflicts. These shifts will not be cost-free. They may, inter alia, prove expensive, affect privacy interests, extend to kinetic operations, and deprive battlefield commanders of options previously available to them. Ultimately, though, law reflects national interests. States will inescapably eventually find it in their interests to take such measures to protect their access to cyberspace and the goods it bestows*. (Schmitt 2014: 299)

On the contrary, the Geneva Centre for the Democratic Control of Armed Forces (DCAF) defines cyberwar as "warlike conduct conducted in virtual space". This is a more inclusive definition that allows the distinction between state-sponsored and non-state-sponsored cyberattacks. It also includes cyber-vandalism, cyber-crime, and cyber-espionage. This perspective links cyberwarfare to cyber-criminality and cyberspace, taking into account all players and intended and unintended effects on non-combatants, the industry and civil society.

CRM could be applied within this broader context as a tool to organise, monitor and control OSINT platforms through a multi-layered governance meta-model. A useful related approach, although more directly addressed to convert OSINT findings into legal evidence, can be found in Gottschalck (2009). Kornmaier and Jaouën (2014) also treat this subject and highlight the emerging role of the individual (2014, 142), trust and cooperative work. We do converge on this perspective:

> *Thus, establishing regulations in strategies and policies for the exchange of information and intelligence in [the above outlined] cyber context is the essential first step in the described process. It must be defined who shares what, with who, under what circumstances, how the information is handled, classified, processed and stored. These regulations are necessary, because on the one hand there exists no broadly accepted standard for sharing information or even intelligence across agencies or private companies. On the other hand – mentioned for completeness – trust is the key for increasing the sharing behaviour. Trust for the exchange occurs at the individual and organizational level. It is the degree of confidence to handle the information/ intelligence with the same sensitivity. Only then the exchange will take place. As well, cooperation between sovereign states is to be fostered for a better efficiency in cyber defence*. (Kornmaier and Jaouën 2014, 152).

9.5.2 Expanding CRM to Cyberwarfare. Ten Preliminary Observations

This is to be read as advance for future work. To broaden the scope of the kind of modelling proposed in this chapter I will depart from the following preliminary observations:

1. The advent of cyberspace has brought new features that make it a unique combat domain. Thus, it raises a governance problem that Schreier (2015, 91), among others, has stated clearly: "*in all states both the decision making apparatus for cyber-attack and the oversight mechanisms for it are inadequate today"*. He points out five distinguishing characteristics: (i) cyberspace has become a "global commons" existing everywhere and open to anyone; (ii) it provides an extended battle space with no real boundaries; (iii) ICT has demolished time and distance in a non-conventional convergence of technologies and infrastructures; (iv) cyberspace favours the attacker; (v) and, fifth, there is a permanent kaleidoscopic change of the components of cyberspace (Schreier 2015, 93).

2. Over 10 years ago, in the aftermath of September 11th in USA, Laura Donohue (2005–06, 1207–8) identified six possibilities in privacy protection to safeguard citizens from invasive ways of surveillance: (i) creating a property right in personal information, (ii) regulating the access, transfer and retention of data while providing remedies for violations, (iii) scaling back the existing powers, (iv) more narrowly defining "national security," (v) creating effective safeguards, (vi) and eliminating clauses that allow for such powers to be "temporary". I don't think things have changed that much. CRM attempts a seventh possibility: creating intermediate institutions to apply the safeguards of global ethics and the Rule of Law while easing security and intelligence services tasks.
3. Balancing cyber security risks against privacy concerns constitute a real challenge. Besides, as stated by Tene (2014, 392–93) "*this delicate balancing act must be performed against a backdrop of laws that are grounded in an obsolescent technological reality. Legal distinctions between communications content and metadata; interception and access to stored information; and foreign intelligence and domestic law enforcement — do not necessarily reflect the existing state of play of the Internet, where metadata may be more revealing than content, storage more harmful than interception, and foreign and domestic intelligence inseparable"* (Tene 2014: 392). Indeed, trying to focus on specific technological functionalities and affordances might facilitate the evaluating task. I do agree with Tene's conclusions: automated monitoring raises less privacy concerns than human observation. This, in turn, implies that the focal point for triggering legal protections should be the moment the system focuses on an individual suspect. This is consistent with Lin et al. suggestion (Lin et al. 2015, 57) to reframing the cybersecurity discussion closer to the individual-actor level.
4. There are striking differences among theoretical proposals to make such a balance. The notions of Data Protection by Design and by Default adopted by the European Union in the General Data Protection Regulation (GDPR) will be eventually enacted in 2016, and will come into force in 2 years. It constitutes an EU strong political bet that is at odds with the strictly liberal legal-market oriented perspective popular among American scholars, where it is assumed that public space is subordinated to private transactions.[19] A quick look to the last European Conferences on Data Protection leads to opposite results: PbD (or DPbD) is the only strategy widely accepted by all participants as a working alternative to generalized surveillance to protect consumers and citizens (Gutwirth et al. 2015).
5. The same difference can be found in legal articles about cloud services and cloud computing. The applicable body of law is separated in two tiers: *primary* privacy law, and *secondary* privacy law. The first one is created by the providers

[19] "*Privacy by design is a system designed not to work […]. The market for consumer privacy has yet to be tested because "privacy by design" policies shift all of the transaction costs of privacy onto consumers. To discover what consumers make of privacy online, the transaction costs of privacy should be shifted from consumers to the owners of internet technology"* (Faioddt 2012, 104-5).

and users of services through privacy contracts, especially, privacy policies. The second one refers to statutes and policies.[20] From this perspective, public space is reduced, and clearly market-driven, *privatised*.

6. In everyday practice, fostering trust is as relevant as reshaping positive or customary international law to adapt norms to this changing digital environment. Therefore, the analytical proposal of a *Meta-rule of law* is entirely compatible with the idea of framing a Global Ethics to handle the fight against cybercrimes, cyberterrorism, and eventually cyberwarfare. This task is far from easy, because terrorist entities and organised crime frequently make use of websites that are beyond the reach of search engines in the so-called "deep" or "dark" Web. Non-indexed sites use a variety of methods to prevent detection from web crawlers —automated browsers that follow hyperlinks, indexing sites for later queries (Morishirna 2012).
7. Human-computer interface could be set as the landmark. Structuring data through second-generation Semantic Web tools starts and ends up into the pragmatic usage of structured information and knowledge in quite different scenarios and environments (Casanovas et al. 2016). Such knowledge can be *personalised*. Likewise, harm caused by worms and malware can reach individuals, groups, communities and political entities at different degrees and levels of granularity. But there is no way to separate casualties from targeted objectives. Civil society, as a whole, is affected. Therefore, any end-user, any member of cyberspace suffers a certain amount of harm. Adding regulations to protections, empowering and controlling LEAs and the military alike, adds normative complexity to the rule of law. Nothing prevents the application of global law to threats, conflicts and wars than can be private and public, virtual and physical at the same time, and most of all occur at the infra- and supra-state level. The Meta-rule of law seems adequate to handle the computer-language levels of contemporary environments, in real settings.
8. From a strictly military standpoint, John Arquilla (2013) recently summarised 20 years of *cyberwar*. Arquilla and Ronfeldt coined the term in a path breaking RAND paper that was published in 1993 in a scholarly journal. Comparing both papers the reader has the impression that Arquilla's original emphasis on the relevance of communications and *knowledge* has been framed later on into two broad and classical fields —war, and justice. *Just war* doctrines —*jus ad bellum*, *jus in bello*, (less) *jus post bellum*. In the middle, military doctrines of fast or attrition war, land vs. sea war, friction (Clausewitz) vs. geometrical (de Jomini) war (Arquilla and Nomura 2015). Thus, the power of nation-states still holds. Something is missing in between, because Arquilla thinks vertically (discourses on war / war of ideas) and horizontally (networked society, "swarm-

[20] "*The secondary privacy law, contained, for example, in statutes and regulations, is for the most part only applicable where no valid privacy contracts exist. This supremacy of privacy contracts over statutory and other secondary privacy law enables individualized privacy protection levels and commercial use of privacy rights according to the contracting parties' individual wish"* (Zimmeck 2012, 451).

ing") about *knowledge*,[21] without exploring its full potential to create self-regulatory institutional bodies, i.e. to reshape the legal landscape in which normative ethics operate. What it should be nuanced is not Arquilla's —and many others'— ideas of war and conflict, but his understanding of how law and regulations operate on and through the Web.

9. This is not saying that the ethical and legal problems pointed out by Arquilla —and many other ethicists— over the evolving cyberspace are not important.[22] They are. He realizes that the temporal sequence ante/and/post war does not represent what really happens in cyber-attacks, where this sequence does not hold. But ethics cannot be reduced to the principles endorsed by customary international law and the Geneva Convention. As I have shown, ethical principles can be embedded and nested on top of the CRM gradual scale to effectively regulate OSINT surveillance and to make the balance with citizens' rights. However, to embrace this point of view, a turning point is needed from a purely positive and normative understanding of law to an intermediate *computational* and *institutional* level. This is directly related to principles and values. E.g. *Fairness* is the tipping point in negotiation and ODR platforms (Casanovas and Zeleznikow 2014). *Accountability* and *transparency* seem to be key in OSINT cybercrime crawling (Casanovas et al. 2014a, 2014b). It is still unclear which ethical values count as the tipping point for justice in OSINT cyberwar crawling. The notion of Meta-rule of law could help thinking at different levels of abstraction (ground, models, meta-models) these ethical concerns, taking specific and situated human/computer interaction as a starting point (Casanovas 2013).
10. There is still room to improve cooperation between NATO and Europol, to put it gently (Rugger 2012). There are striking differences between USA and EU legal and policy strategies. The European Cybercrime Centre (EC3) commenced its activities in January 2013 at Europol.[23] Europol became an autonomous European agency in January 2010. Since then, cooperation among EU agencies is a fact (e.g. between Europol and Eurojust). But this does not hold for all state-members, especially in the counterterrorism area. Political and organizational barriers are still in place. The common USA-EU Safe Harbor Agreement has been replaced by the Privacy Shield policy on transatlantic

[21] "Swarming" means "simultaneous attack from many directions". See about the military development of cyberwarfare and the two competing paradigms of "*strategic information warfare as launching 'bolts from the blue' and cyberwar as doing better in battle strategic warfare"*, Arquilla (2011, 60).

[22] "*(…) it seems that a kind of ethical 'bottom line' assessment might be discernible about cyberwar, in two parts. First*, jus ad bellum *comes under great pressure in the key areas of right purpose, duly constituted authority, and last resort. However, the apparent benefits of waging preventive or pre-emptive war, concepts with a lineage dating from Thucydides and Francis Bacon,10 are largely illusory. Second, it seems that* jus in bello *considerations come off rather better in the areas of proportionality and non-combatant immunity although there is a bit of complexity in the parsing of notions of acceptable"* (Arquilla 2013, 85).

[23] https://www.europol.europa.eu/ec3

dataflows,[24] still under discussion.[25] This failure to cooperate presents several features: (i) disparities in the political, administrative and judicial frameworks of EU Member States obstruct effective information sharing and coordination; (ii) disparities between intelligence and police agencies arise because counter-terrorism issues are shared by organizations with mismatched interests; (iii) disparities in priorities and values; (iv) most important, disparities at the semantic interoperability level of the main legal and criminal concepts. This is an additional reason to think carefully and adopt the Meta-rule of law proposed in this chapter.

Acknowledgments This research has been funded by the F7 EU Project *Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime* (CAPER) —Grant Agreement 261712—; and by the National Project *Crowdsourcing*, DER2012-39492-C02-01 and the Australian project D2D CRC.

References

Albrecht, P. 2015. EU general data protection regulation: The outcome of the negotiations ("trilogues") and 10 key points. Lead European Parliament Committee: Committee on Civil Liberties, Justice and Home Affairs (LIBE). 17 December. http://www.janalbrecht.eu/fileadmin/material/Dokumente/20151217_Data_protection_10_key_points_EN.pdf Accessed 21 May 2016.

Aldrich, J.H. 2010. Elinor Ostrom and the "just right" solution. *Public Choice* 143: 269–273. doi:10.1007/s11127-010-9630-9.

Aligica, P.D., and P. Boettke. 2011. The two social philosophies of Ostroms' institutionalism. *The Policy Studies Journal* 39(1): 29–49. doi:10.1111/j.1541-0072.2010.0000395.x.

Aliprandi, C., J.A. Irujo, M. Cuadros, S. Maier, F. Melero, and M. Raffaelli. 2014. CAPER: Collaborative information, acquisition, processing, exploitation and reporting for the prevention of organised crime. *HCI* 26: 147–152.

Arquilla, J. 2011. From *blitzkrieg* to *bitskrieg*: The military encounter with computers. *Communications of the ACM* 54(10): 58–65. doi:10.1145/2001269.2001287.

Arquilla, J. 2013. Twenty years of cyberwar. *Journal of Military Ethics* 12(1): 80–87. doi:10.1080/15027570.2013.782632.

Arquilla, J., and D. Ronfeldt. 1993. Cyberwar is coming! *Comparative Strategy* 12(2): 141–165. Rand Corporation. http://www.rand.org/pubs/reprints/RP223.html. Accessed 21 May 2016.

Arquilla, J., and R. Nomura. 2015. Three wars of ideas about the idea of war. *Comparative Strategy* 34(2): 185–201.

Article 29 Working Party. 2014a. Joint statement of the European data protection authorities assembled in the Article 29 working party, November 25th (adopted on 26th). http://ec.europa.

[24] http://europa.eu/rapid/press-release_IP-16-216_en.htm

[25] Cfr. the Article 29 Data Protection Working Party *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, a*dopted on 13 April 2016*: "*The check and controls of the adequacy requirements must be strictly performed, taking into account the fundamental rights to privacy and data protection and the number of individuals potentially affected by transfers. The Privacy Shield needs to be viewed in the current international context, such as the emergence of big data and the growing security needs*".

eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf. Accessed 21 May 2016.

Article 29 Working Party. 2014b. Working document on surveillance of electronic communications for intelligence and national security purposes, adopted on December 4th, 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf. Accessed 21 May 2016.

Article 29 Working Party. 2016. Article 29 Data protection working party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf Accessed 21 May 2016.

Backfried, G., C. Schmidt, M. Pfeiffer, G. Quirchmayr, M. Markus Glanzer, and K. Rainer. 2012. Open source intelligence in disaster management. 2012 European Intelligence and Security Informatics Conference, EISIC. *IEEE Computer Society* 254–258.

Best, C. 2008. Open source intelligence. In *Mining massive data sets for security: advances in data mining, search, social networks and text mining, and their applications to security*, ed. F. Fogelmann-Soulié et al. 19: 331–344. Amsterdam: IOS Press.

Best, R., and A. Cumming. 2008. Open Source Intelligence (OSINT): Issues for Congress, *CRS Report for Congress*, Order Code RL34270, Updated January 28 2008. https://www.fas.org/sgp/crs/intel/RL34270.pdf. Accessed 21 May 2016.

Bradbury, D. 2011. In plain view: Open source intelligence. *Computer Fraud & Security* 4**:** 5–9**.** Elsevier https://www.cse.msu.edu/~enbody/CFS_2011-04_Apr.pdf. Accessed 21 May 2016.

Burdon, M. 2010. Privacy Invasive Geo-mashups. Privacy 2.0 and the Limits of First Generation Privacy Law. *University of Illinois Journal of Law, Technology and Policy* 1: 1–50.

Burke, C. 2007. Freeing knowledge, telling secrets: Open source intelligence and development. *CEWCES Research Papers.* Paper 11. http://epublications.bond.edu.au/cewces_papers/11. Accessed 21 May 2016.

Cameron, K. 2005. The laws of identity …as of 5/11/2005. Microsoft Corporation, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf Accessed 21 May 2015.

Casanovas, P. 2013. Agreement and relational justice: A perspective from philosophy and sociology of law. In *Agreement Technologies*, ed. Sascha Ossowski, LGTS 8, Springer Verlag, 19–42, Dordrecht/Heidelberg: Springer. doi:10.1007/978-94-007-5583-3.

Casanovas, P. 2014. Open source intelligence, Open social intelligence, and privacy by design. European conference on social intelligence. *Proceedings of the European Conference on Social Intelligence (ECSI-2014)*, eds. Andreas Herzig and Emiliano Lorini, 174–185. Barcelona, Spain, November 35, 2014, CEUR http://ceur-ws.org/Vol-1283/ Accessed 21 May 2016.

Casanovas, P. 2015a. Semantic web regulatory models: Why ethics matter, special issue on information society and ethical inquiries. *Philosophy & Technology* 28(1): 33–55. doi:10.1007/s13347-014-0170-y.

Casanovas, P. 2015b. Conceptualisation of rights and meta-rule of law for the web of data. *Democracia Digital e Governo Eletrônico* 1(12): 18–41. http://buscalegis.ufsc.br/revistas/index.php/observatoriodoegov/article/view/34399. Accessed 21 May 2016. Reprinted in *Journal of Governance and Regulation* 4(4): 118–129.

Casanovas, P., Casellas, N., Tempich, C. et al. 2007. *Artificial Intelligence and Law* 15: 171. doi:10.1007/s10506-007-9036-2

Casanovas, P., and J. Zeleznikow. 2014. Online dispute resolution and models of relational law and justice: A table of ethical principles. In *AI approaches to the complexity of legal systems IV. social intelligence, models and applications for law and justice systems in the semantic web and legal reasoning*, ed. P. Casanovas et al., LNAI 8929, 55–69. Heidelberg/Berlin: Springer.

Casanovas, P., E. Teodoro, R. Varela, J. González-Conejero, and A. Roig, et al. 2014a. *D 7.8 EAG ethical report code. Final ethical audit on system development and deployment*, EU F7 CAPER, FP7-SECURITY-2010-1.2-1, 24/10/2014.

Casanovas, P., J. Arraiza, F. Melero, J. González-Conejero, G. Molcho, and M. Cuadros. 2014b. Fighting organized crime through open source intelligence: Regulatory strategies of the

CAPER project. In *Legal knowledge and information systems. JURIX 2014: The twenty-seventh annual conference*, Foundations on artificial intelligence, 271, ed. Rinke Hoekstra, 189–199, Amsterdam: IOS Press.

Casanovas, P., M. Palmirani, S. Peroni, T. van Engers, and F. Vitali. 2016. Special issue on the semantic web for the legal domain guest editors' editorial: The next step. *Semantic Web Journal* 7(3): 213–227. IOS Press. http://www.semantic-web-journal.net/system/files/swj1344.pdf. Accessed 21 May 2016.

Casellas, N., M. Blázquez, A. Kiryakov, P. Casanovas, M. Poblet, R. Benjamins. 2005. OPJK into PROTON: Legal domain ontology integration into an upper-level ontology. *On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops*, ed. R. Meersman et al., LNCS 3762, 846–855. Berlin/Heidelberg: Springer.

Castelfranchi, C. 2014. Minds as social institutions. *Phenomenology and Cognitive Science* 13(1): 121–143. doi:10.1007/s11097-013-9324-0.

Cavoukian, A. 2010. *Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices. Information and privacy commissioner*. Ontario, Canada. http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/. Accessed 21 May 2016.

Cavoukian, A. 2012. Privacy by design. *IEEE Technology and Society Magazine* 4: 18–19. doi:10.1109/MTS.2012.2225459. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6387956. Accessed 21 May 2016.

Ciambra, A., and P. Casanovas. 2014. Drafting a composite indicator of validity for regulatory models and legal systems. In *AI approaches to the complexity of legal systems IV. Social intelligence, models and applications for law and justice systems in the semantic web and legal reasoning*, ed. P. Casanovas et al., 70–82. LNAI 8929, Heidelberg/Berlin: Springer.

Colesky, M., Hoepman, J. H., Hillen, C. A. 2016. Critical Analysis of Privacy Design Strategies. IEEE Symposium on Security and Privacy Workshops, 33–40.

de Hert, P. and Papakonstantinou, V., 2016. The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review*, 32 (2): 179–194.

Donohue, L.K. 2005-2006. Anglo-American Privacy and Surveillance. *Journal of Criminal Law and Criminology* 93 (3): 1059–1208.

EGE. 2014a. Ethics of security and surveillance technologies, Opinion no. 28 of the European Group on Ethics in Science and new Technologies, Brussels, 20 May 2014, http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf Accessed 21 May 2016.

EGE. 2014b. Press release on the EGE opinion 28, of 20 May 2014. http://ec.europa.eu/bepa/european-group-ethics/docs/publications/press_release_ege_opinion_28_.pdf. Accessed 21 May 2016.

EU Commission. 2014. Progress on EU data protection reform now irreversible following European Parliament vote European Commission – MEMO/14/186 12/03/2014, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm. Accessed 21 May 2016.

Faioddt, J.T. 2012. Mixed reality: How the laws of virtual worlds govern everyday life. *Berckeley Technology Law Journal* 27 1/3: 55–116. doi:10.15779/Z38ST2W.

Fleisher, C. 2008. OSINT: Its implications for business/CompetitiveIntelligence analysis and analysts, OSINT: Its implications for business/competitive intelligence analysis and analysts. *Inteligencia y Seguridad* 4: 115–141. http://www.phibetaiota.net/wp-content/uploads/2013/02/2008-Fleisher-on-OSINT-English-and-Spanish.pdf. Accessed 21 May 2016.

Floridi, L., and M. Taddeo (eds.). 2014. *The ethics of information warfare*, LGTS 14. Heidelberg/Dordrecht: Springer.

Glassman, M., and M.J. Kang. 2012. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior* 28: 673–682. doi:10.1016/j.chb.2011.11.014.

González-Conejero, J., R. Varela-Figueroa, J. Muñoz-Gómez, and E. Teodoro. 2014. Organized crime structure modelling for European law enforcement agencies interoperability through

ontologies. In *AI approaches to the complexity of legal systems. AICOL IV-V*, ed. P. Casanovas, U. Pagallo, M. Palmirani, and G. Sartor, 217–231. LNAI 8929. Heidelberg, Dordrecht: Springer. doi: 10.1007/978-3-662-45960-7_16.

Gottschalck, P. 2009. Information sources in police intelligence. *The Police Journal* 82: 149–170. doi:10.1350/pojo.2009.82.2.463.

Gutwirth, S., R. Leenes, P. de Hert (eds.). 2015. *Reforming European data protection law*, LGTS, Dordrecht/Heidelberg: Springer. doi:10.1007/978-94-017-9385-8.

Hoepman, J.H. 2014. Privacy design strategies (extended abstract). In ICT systems security and privacy protection. *29th IFIP TC 11 International Conference, SEC 2014*, *Marrakech, Morocco, June 2-4*, Proceedings. *IFIP Advances in Information and Communication Technology*, ed. N. Cuppens-Boulahia et al., 446–459. Heidelberg: Springer.

Jardines, E.A. 2015. Open source intelligence. In *The five disciplines of intelligence collection*, ed. Mark M. Lowenthal and Robert M. Clark, chapt.2, L.A., Washington: CQ Press.

Keane, J., and P. Bell. 2013. Confidence in the police: Balancing public image with community safety. A comparative review of the literature, *International Journal of Law, Crime and Justice* 41: 233–246. doi:10.1016/j.ijlcj.2013.06.003.

Kilovaty, I. 2014. Cyber warfare and the Jus Ad Bellum challenges: Evaluation in the light of the Tallinn manual on the international law applicable to cyber warfare. *National Security Law Brief* 5(1): 91–124. http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1066&context=nslb. Accessed 21 May 2016.

Kim, Y., M. Glassman, M. Bartholomew, and E.H. Hur. 2013. Creating an educational context for open source intelligence: The development of internet self-efficacy through a blogcentric course. *Computers & Education* 69: 332–342. doi:10.1016/j.compedu.2013.07.034.

Koops, B.-J., J.H. Hoepman, and R. Leenes. 2013. Open-source intelligence and privacy by design. *Computer Law & Security Review* 29: 676–688. doi:10.1016/j.clsr.2013.09.005.

Koops, B-J., and R. Leenes. 2014. Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology* 28(2): 159–171. doi:10.1080/13600869.2013.801589.

Kornmaier, A., and F. Jaouën. 2014. Beyond technical data -a more comprehensive situational awareness fed by available intelligence information. *2014 6th International Conference on Cyber Conflict*, ed. P. Brangetto, M. Maybaum, and J. Stinissen, 139–156, NATO CCD COE Publications. https://ccdcoe.org/sites/default/files/multimedia/pdf/d0r0s2_kornmeier.pdf. Accessed 21 May 2016.

Kshetri, N. 2010. *The global cybercrime industry. Economic, institutional and strategic perspectives.* Heidelberg/Dordrecht: Springer.

Lessig, L. 2006. *Code* and *other laws of cyberspace* (2001), *Code 2.0* (2006). Crowdourced version. http://codev2.cc/ Accessed 21 May 2016.

Lin, P., P. Allhoff, and K. Abney. 2015. Is warfare the right frame for the cyber debate? In *The ethics of information warfare*, ed. L. Floridi and R. Taddeo, 39–57. LGTS, Dordrecht/Heidelberg: Springer. doi:10.1007/978-3-319-04135-3.

McCary, M. 2013. Sun Tzu's battle for our footnotes: the emergent role of libraries in juridical warfare. *University of Miami National Security & Armed Conflict Law Review* 3(Fall): 46–103. http://www.m2lawpc.com/index_htm_files/McCary-Sun%20Tzu%20Footnotes-UM-NSAC%20L%20Rev-Vol-III-2013.pdf Accessed 21 May 2016.

Moshirnia, A.V. 2012. Valuing speech and open source intelligence in the face of judicial deference. *Harvard National Security Journal* 4(2012-3): 385–454. http://harvardnsj.org/wp-content/uploads/2013/05/Vo.4-Moshirnia-Final.pdf. Accessed 21 May 2016.

Murkens, J.E.M. 2007. The future of *Staatsrecht:* Dominance, demise or demystification? *The Modern Law Review* 70(5): 731–758. doi:10.1007/978-3-540-73810-7_2.

Noriega, P., and M. d'Inverno. 2014. Crowd-based socio-cognitive systems. In *Crowd intelligence: Foundations, methods and practices. European network for social intelligence*, ed. M. Poblet, P. Noriega, and E. Plaza, Barcelona, January 2014, http://ceur-ws.org/Vol-1148/CROWD2014 Accessed 21 May 2016.

Noriega, P., J. Padget, H. Verhagen, and M. d'Inverno. 2014. The challenge of artificial socio-cognitive systems. In AMMAS 14' Proceedings. http://aamas2014.lip6.fr/proceedings/workshops/AAMAS2014-W22/p12.pdf. Accessed 21 May 2016.

O'Connor, T.R. 2006. Intelligence-led policing and transnational justice. *Journal of the Institute of Justice & International Studies* 6: 233–239.

Orend, B. 2014. Fog in the fifth dimension: The ethics of cyber-war. In *The ethics of information warfare*, ed. L. Floridi and R. Taddeo, 1–23. Dordrecht/Heidelberg: Springer. doi:10.1007/978-3-319-04135-3.

Ostrom, E. 2010. Institutional analysis and development. Micro *workshop in political theory and political analysis. Proceedings of the policy studies organization*, New series 9, 851–878 http://www.ipsonet.org/proceedings/category/volumes/2010/no-9/ Accessed 21 May 2016.

Palombella, G. 2009. The rule of law beyond the state: Failures, promises, and theory. *International Journal of Constitutional Law* 7(3): 442–467. doi:10.1093/icon/mop012.

Palombella, G. 2010. The rule of law as institutional ideal. *Comparative Sociology* 9: 4–39. doi:10.1163/156913210X12535202814315.

Phythian, M. 2009. Intelligence analysis today and tomorrow. *Security Challenges* 5(1): 69–85. doi:10.1080/13619462.2014.987530.

Poblet, M. (ed.). 2011. *Mobile technologies for conflict management. Online dispute resolution, governance, participation*. LGTS, Dordrecht/Heidelberg: Springer. doi:10.1007/978-94-007-1384-0.

Poblet, M. 2013. Visualizing the law: Crisis mapping as an open tool for legal practice. *Journal of Open Access to Law* 1. Ithaca, Cornell: https://ojs.law.cornell.edu/index.php/joal/article/viewFile/12/13 Accessed 21 May 2016.

Poblet, M., E. García-Cuesta, and P. Casanovas. 2014. Crowdsourcing tools for disaster management: A review of platforms and methods. In *AI approaches to the complexity of legal systems IV. Social intelligence, models and applications for law and justice systems in the semantic web and legal reasoning*, ed. P. Casanovas et al., 262–276. LNAI 8929, Dordrecht, Heidelberg: Springer. doi: 10.1007/978-3-662-45960-7_19.

Ratcliffe, J.H. 2003. Intelligence-Led policing. *Trends and issues in crime and criminal justice*, 248. Canberra: Australian Institute of Criminology.

Ratcliffe, J.H. 2008. *Intelligence-led policing*. Cullompton: Willan Publishing.

Risch, J.M. 2009. Virtual rule of law. *West Virginia Law Review* 112(1): 1–50.

Robson, T.A. 2009. A burning need to know: the use of open source intelligence in the Fire Service. Thesis. Monterrey: Naval School. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.6834&rep=rep1&type=pdf Accessed 21 May 2016.

Rodriguez-Doncel, V., C. Santos, P. Casanovas, and A. Gómez-Pérez. 2016. Legal aspects of linked data – The Europeanframework, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.07.005

Rugge, F. 2012. The case for NATO-EU cooperation in the protection of cyberspace. In *Cybersecurity Summit (WCS), 2012 Third Worldwide*, 1–10. IEEE.

Schmitt, M.N. (ed.). 2013. *Tallinn manual on international law applied to cyber warfare*. Cambridge: Cambridge University Press.

Schmitt, M.N. 2014. The law of cyber warfare: Quo Vadis. *Stanford Law and Policy Review* 25: 269–300.

Schmitt, M.N., and S. Watts. 2014. The decline of international humanitarian Law Opinio Juris and the law of cyber warfare. *Texas International Law Journal* 50: 189–231.

Schreier, F. 2015. On cyberwarfare. *DKAF Horizon* 2015, WP 7. http://docplayer.net/4159538-Dcaf-horizon-2015-working-paper-no-7-on-cyberwarfare-fred-schreier.html Acessed 21 May 2016.

Solis, G. 2014. Cyberwarfare. *Military law review*, 219(Spring): 1–52. http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/219-spring-2014.pdf Accessed 21 May 2016.

Steele, R.D. 2007. Open source intelligence. In *Handbook of intelligence studies*, ed. Loch Johnson, 129–147, New York: Routledge.

Taddeo, M. 2012. Information warfare: a philosophical perspective. *Philosophy & Technology* 25.1(2012): 105–120. doi: 10.1007/s13347-011-0040-9.

Tamanaha, B. 2011. The rule of law and legal pluralism in development. *Hague Journal on the Rule of Law* 3: 1–17. doi: http://dx.doi.org/10.1017/S1876404511100019.

Tene, O. 2014. A new Harm Matrix for cybersecurity surveillance. *Colorado Technology Law Journal* 12(2): 391–426.

Trottier, D. 2014. Police and user-led investigations on social media. *Journal of Law, Information and Science* 23: 75–96. AustLII: http://www.austlii.edu.au/au/journals/JlLawInfoSci/2014/4.html Accessed 21 May 2016.

Usmani, Z-ul-H. 2014. Predictive modeling to counter terrorist attacks. *Go-FigSolutions* An Interview with Max Ernst, Pranav Sharma, and Neil Singh, Providence, RI, 9 February.

Verfaille, K., and T.V.d. Beken. 2008. Proactive policing and the assessment of organised crime. *Policing. An International Journal of Police Strategy and Management* 31(4): 534–552. doi: 10.1108/13639510810910553.

Zeadally, S., and A. Flowers. 2014. Cyberwar: The what, when, why, and how [commentary]. *Technology and Society Magazine, IEEE* 33(3): 14–21. doi:10.1109/MTS.2014.2345196.

Zimmeck, S. 2012. The information privacy Law of Web applications and cloud computing. *Santa Clara Computer & High Technology Law Journal* 29: 451–487.

Zittrain, J.L. 2008. *The future of the internet – And how to stop It*. New Haven/London: Yale University Press & Penguin UK. Harvard University's DASH Repository. http://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future%20of%20the%20Internet.pdf?sequence=1. Accessed 21 May 2016.

Pompeu Casanovas is director of advanced research, professor of philosophy and sociology of law at the Autonomous University of Barcelona (Spain) and adjunct professor at Royal Melbourne Institute of Technology (RMIT, Australia). He is serving as head of the UAB Institute of Law and Technology as well. He is general coeditor of the Springer Law, Governance and Technology Series (Germany) and coeditor of the *Journal of Open Access to Law* at the University of Cornell (USA).