Enhancing the effectiveness of cybercrime prevention through policy monitoring

Benoît Dupont, Université de Montréal[1]

Published as :
B. Dupont (2019), Enhancing the effectiveness of cybercrime prevention through policy monitoring, *Journal of Crime and Justice*, 42 (5), 500-515. doi: 10.1080/0735648X.2019.1691855.

Abstract:

This article examines the feasibility of designing and implementing a cybercrime prevention monitoring approach to enhance the quality of knowledge about policies that aim to reduce the prevalence and impact of online harms. Despite very significant investments made by governments over the past decade to improve the cybersecurity of publicly and privately-operated computer systems, there is very limited systematic knowledge about what cybercrime prevention policies have been adopted in various parts of the world and even less knowledge about their effectiveness in reducing the exposure of individuals and organizations to cybercrime. Borrowing from the policy monitoring (or policy surveillance) methodology that was developed in a broad range of fields such as public health and education, this article argues that such an approach would be critical in advancing our understanding of what is being done to control cybercrime, what works, what doesn't, and what is promising. This article provides an overview of the principles and benefits of the policy monitoring approach, reviews the main features of a sample of 18 policy monitoring platforms, assesses a dozen cybersecurity policy rating initiatives—concluding that very few of them include cybercrime in their framework, then provides a template for the creation of a dedicated cybercrime prevention monitoring tool that would benefit academics, policy-makers and practitioners.

Keywords: Policy monitoring, cybercrime prevention, evidence-based cybersecurity

[1] I would like to acknowledge the financial support received from the Korean Institute of Criminology, which made this research possible, as well as the remarkable research assistance provided by Elsa Euvrard, Chloé Majdalany, Shannon McPhail, and Michael Joyce. All errors and omissions remain my own.

Introduction

The statistics available on cybercrime, although imprecise and fragmentary (Florêncio and Herley 2013, Furnell et al. 2015, Levi 2017, Reep-van den Bergh and Junger 2018), are staggering. In 2014, the Center for Strategic and International Studies (CSIS), in a report sponsored by the security firm McAfee, estimated that cybercrime and espionage cost $445 billion annually worldwide (CSIS 2014). In 2015 the insurance company Lloyd's arrived at almost the same number ($400 billion a year) for the costs of cyber-attacks and the disruptions they cause to businesses (Gandel 2015). A more cautious and conservative assessment, made by a group of computer scientists and criminologists who extrapolated their numbers from U.K. data, suggests that the global cost of cybercrime during the 2010s could reach $75 billion—$225 billion if traditional crimes that are transitioning to cyber are included (Anderson et al. 2013). In Canada, one of the most recent and comprehensive surveys, conducted in 2017 with a representative sample of 10,000 businesses, found that companies of all sizes had spent Can$14 billion over the previous year to protect their systems against various forms of online harm, and that over one fifth of them had been impacted by a cybersecurity incident (Bilodeau et al. 2019). As a result, cyber-risks have topped the list of security concerns for government and business leaders in the past few years and even more disruptive outcomes are anticipated as our societies become increasingly cyber-dependent and interconnected (WEF 2017, Zurich 2014). Despite the global scope and impact of cybercrime, few tools are available to assess effective policies for reducing cybercrime. This study fills this gap in the literature.

The figures on cybersecurity are also striking. The global market for cybersecurity products and services is estimated to have reached $120 billion in 2017, a 35-fold increase over the past 13 years, with a predicted growth rate of 12-15% until 2021 (Cybersecurity Ventures 2017). Gartner (2017), a widely cited consultancy, produced a more conservative assessment, with a worldwide spending estimate of $86.4 billion for 2017 and 7% annual growth. These numbers are impressive in the current economic context where slow growth has become the norm for Western economies. In addition, recent events in the U.S., the U.K., France, and approximately 40 other nations have shown that cyber threats can move beyond critical infrastructures and online financial services to target electoral processes and undermine trust in democratic institutions (CSE 2017).

In response to this fast-changing risk landscape, governments across the world are designing cybersecurity policies and allocating billions of dollars of their defense and R&D budgets to new programs that will enhance their ability to address cyber risks. The U.S. federal government, for example, will spend almost $16.6 billion in 2019 on cybersecurity (The White House 2019). In the U.K., in November 2015 the chancellor announced cybersecurity investments of £1.9 billion over five years, which will bring the government's overall commitment for cybersecurity to £3.2 billion (Osborne 2015). Australia, a middle power, announced a comprehensive cybersecurity strategy in 2016 with allocations of AU$230 million over five years (Duckett 2016). The European Union has focused its cybersecurity investments on R&D with a plan to fund businesses and universities to the extent of €450 million over four years (2017 to 2020), with public-private collaborations expected to leverage three times more in matching funds (European Commission 2016).

Despite these massive investments in cybercrime-prevention and cybersecurity policies, very few tools are available to help policy makers and the public determine the effectiveness of government interventions against online harms. This article examines the potential of policy

monitoring tools to fill this gap. Policy monitoring is an evidence-based approach developed by public policy scholars as a way to assess and compare the effectiveness of laws and policies. It relies on systematic collection of data on the design and implementation of policies, rigorous evaluation of their impact, and wide dissemination of these assessments. This article argues that a policy monitoring platform could encourage the creation of a more robust knowledge base about the cybercrime prevention initiatives being developed around the world, in order to facilitate the dissemination of effective policies and discourage the adoption of counterproductive interventions.

I discuss the rationale and need for a policy monitoring approach in the field of cybercrime prevention in the first section and introduce its main principles in the second section. The third section reviews a small sample of established policy monitoring platforms to identify their main features, as well as their limitations. I then focus on half a dozen cybersecurity rating initiatives that attempt to assess the efforts of various countries and international organizations to mitigate cyber-harms, highlighting not only their strengths but also their relative lack of importance for cybercrime prevention policies. Finally, I explore why criminologists should consider establishing a cybercrime prevention monitoring platform and how such a platform could operate. This article is more a call to action to cybercrime researchers and practitioners to enhance the quality of their knowledge about what exists and what works in cybercrime prevention than a traditional theoretical or empirical contribution about a specific type of cybercrime and the public and private responses to it.

1. The need for more systematic tracking of cybercrime prevention policies and programs

The numbers cited in the introduction reflect only a fraction of the significant budgets allocated by governments, international organizations, and businesses in attempts to address the complex problems created by cybercrime. Unfortunately there is no source of consolidated data that would make it possible to measure and track these efforts at global, national, or even local levels, nor is there a centralized database of the various policies and programs implemented by public, private, and community stakeholders. This lack of information, in a budgetary context where the billions of dollars now being spent on cybersecurity will increase at a steady pace for the next few years, is problematic for three main reasons.

First, it prevents us from systematically and empirically assessing the nature, effectiveness, and efficiency of the various cybercrime prevention programs that are being developed and implemented across the world (Hutchings and Holt 2017). A few criminological studies have attempted to evaluate the deterrence effects of warning banners on attacked computer systems (Maimon et al. 2014), the protective effects of using financial intelligence to warn potential online fraud victims (Cross 2016), and the disruptive and mitigating effects generated when large software companies and Internet Service Providers combat botnets (Dupont 2017). However each of these studies not only focused on a specific form of cybercrime and intervention strategy but also adopted a different methodology, making comparisons difficult. The lack of a common framework for tracking cybercrime prevention policies and their innovative features—which would be a first step towards a more rigorous measurement of their impact (for instance whether they achieve their objectives at a reasonable cost)—severely limits the evidence base for determining which approaches work, do not work, or are promising (Sherman et al. 1997). Making

important decisions on flimsy evidence creates the risk that ineffective programs will receive undue attention and investments while proven strategies are ignored.

Second, at the international level, this lack of baseline information restricts the dissemination of knowledge and both impedes the adoption of policies that have been proven to deliver positive outcomes and prevents the debunking of failed or counterproductive policies. Lessons learned locally are not shared globally, although cybercrime problems are very similar across countries at comparable stages of economic and technological development. A more sustained and systematic knowledge transfer effort could help both mature and emerging digital economies share the benefits of a safer online ecosystem.

Finally, the absence of a common framework for analyzing cybercrime prevention policies hinders coordination efforts that could deliver more effective responses to transnational cybercrime and cyber-risks. While international organizations such as the International Telecommunications Union and Interpol or European agencies such as Europol and ENISA have all started to develop ambitious capacity-building initiatives to support developed and developing countries in their efforts to protect their citizens against cyber harms, the absence of systematic knowledge about which policies are already being implemented by which countries, at what cost, and with what results reduces the opportunities for policy harmonization and synchronization.

Cybercrime is not the only policy domain in which there is a lack of integration in the information needed to facilitate the implementation of effective or promising policies and intervention strategies in diverse local and national contexts. Complex policy domains such as public health, education, environmental protection, urban planning, and criminal justice have all attempted to address similar information deficits by developing *policy monitoring* or *policy surveillance* methodologies. (Although the two terminologies may appear different, they reflect very similar objectives and outcomes and are used interchangeably in this article.)

2. Policy surveillance: definition and principles

Policy surveillance can be defined as "the systematic collection, analysis and dissemination of information about laws and other policies" (Chriqui et al. 2011: 21). Its main objective is to learn "which policy-making entities are doing what through 'mapping studies' that capture the content and variation of policies across jurisdictions or institutions" (Burris et al. 2016: 1063). Such surveillance differs from more classical policy analysis in its scientific design, which includes rigorous protocols that support the monitoring process and specify the laws and policies of interest, outlines of inclusion and exclusion criteria, acknowledgment of search methodologies and their limits, and quantitative and qualitative coding schemes that minimize analyst subjectivity (Burris et al. 2010: 182). Policy surveillance adopts a dynamic approach through regular updates to the data as tracking the progress of policies at specific reference dates or intervals makes longitudinal analyses of outcomes and impacts possible (Burris et al. 2016: 1069).

Policy surveillance is heavily influenced by its research focus: its core objective is to facilitate the implementation of effective policies that can benefit the common good and to do so by laying the foundation for impact studies that evaluate the effectiveness of a broad range of options. By making their datasets publicly available (usually through websites) and providing stakeholders and the general public with powerful search and visualization tools, policy monitoring initiatives hope not only to foster research projects that can evaluate important policies at reduced costs but also to make it simpler for policymakers and end users to understand the large number of policies and

key subcomponents relevant to their area of interest and to increase their analytical and innovation capacities (Burris et al. 2016: 1070). This systematic approach to the creation of transferable and assessable knowledge is particularly important when policy domains are heavily influenced by opinion, politics, and hype, as is the case for cybercrime and cybersecurity (Lee and Rid 2014).

As monitoring resources are finite, it is important to recognize that not all policies deserve to be systematically documented. Presley et al. (2015: 55-56) suggest five criteria, listed here in order of decreasing importance, to help researchers select the most relevant policies. Although these criteria originate in the public health field, they are general enough to apply to most other policy domains:

1. Significance of the problem (policy deals with a pressing issue);
2. Salience (policy reflects the aggregate interest of a broad range of stakeholders);
3. Existence of evidence or evaluation (prioritizes evaluation of policies that have been widely adopted but not yet evaluated);
4. Adopted as a national priority (policy affects how national strategies are implemented and translated into measurable programs);
5. Determination of cost (cost of policy surveillance varies greatly depending on information accessibility and complexity).

3. Existing policy surveillance platforms

One indicator of policy surveillance's usefulness to decision makers is its growth in popularity over the past few years. For example, Presley et al. (2015: 41-51) list more than 160 U.S. surveillance resources that follow policies in domains as diverse as tobacco control, school nutrition, anti-bullying, immigration, and climate change, among others. International organizations such as the International Labor Organization and the World Health Organization also track policy surveillance tools that facilitate global comparisons (Burris et al. 2016: 1071). The Campbell Collaboration, an international clearinghouse that promotes evidence-based policies and practices, lists more than two dozen evidence portals that provide policy monitoring functions[2].

In order to better understand how policy surveillance platforms are developed and maintained, and what kind of data they provide their users, an extensive literature review was conducted. Eighteen policy surveillance platforms that had been examined in depth were identified and the organization and availability of their data online was analyzed. The policy monitoring tools used by these platforms are described in Table 1.

INSERT TABLE 1 ABOUT HERE

Systematic analysis of these platforms was performed to understand how they generate value for their users and for policy makers. Eight key dimensions that seem particularly relevant to the implementation of a policy monitoring approach to cybercrime prevention were identified and coded, making it possible to highlight the incidence of certain features.

[2] https://www.campbellcollaboration.org/better-evidence/evidence-portals.html.

1. Policy surveillance tools are most developed in public health: policy surveillance thrives in fields of study where evidence-based approaches are well established: public health accounts for 72% of the sample, followed by crime and justice (17%), youth development (6%), and cross-sectoral (6%) platforms.
2. Policy surveillance tools are jointly developed by public agencies and non-profits: Leadership in creating and maintaining these monitoring tools is shared between public sector agencies (50%) and non-profits and NGOs such as academic institutions and non-profit foundations (39%), with the remaining 11% reflecting joint efforts by these two groups.
3. Policy surveillance tools are most developed in the US and focus more on geographical than on temporal comparisons: The sample described here is very U.S. centric, with more than half the platforms reviewed comparing legislation, policies, and programs across American municipalities and states (56%) while only one platform (6%) provides international comparative data. Policies are described as isolated initiatives in 39% of the reviewed databases, although many policies and programs are delivered as part of complex national or local strategies involving multiple approaches. Only two platforms (crimesolutions.gov and coalition4evidence.org) provide multiple evaluation results that can be compared and averaged out for each selected program to account for the various levels of scientific rigour that characterize evaluative studies carried out by different teams in different settings. Finally, only 28% of the reviewed platforms track and compare policies and legislation over time, making it possible to account for variations and stability.
4. Policy surveillance tools rely on secondary data: in terms of data sourcing, all of the reviewed platforms (100%) use data and information produced by third parties, such as program implementation agencies, official statistical sources, or independent evaluators. The costs of collecting data or conducting evaluations independently appear to be prohibitive, which means that the quality and integrity of the secondary data used by these platforms needs to be thoroughly assessed.
5. All policy surveillance tools are based on literature reviews: as a direct consequence of the aggregation approach highlighted above, all platforms (100%) rely on literature reviews for descriptions and evaluations of the policies and programs they include in their databases. The depth of these literature reviews varies greatly: while certain platforms provide long lists of peer-reviewed references for every program included in their database, others prefer to focus on a limited number of studies (usually one or two) that provide the most detailed description or evaluation of a policy or program's outcomes. In less mature policy fields, monitoring platforms must rely on official reports, usually produced by program implementers, or on articles published in professional or mainstream media.
6. Only slightly more than half of policy surveillance tools (56%) provide evaluation outcomes for the policies or programs they include. The remaining 44% focus on comprehensive descriptions of local legislative or policy frameworks in the hope that this formatted data will be useful to future independent evaluators. Most platforms that rate the effectiveness of policies use the 'gold standard' of Randomized Control Trials (RCTs) as their main criteria (Sampson 2010; Bothwell et al. 2016; Fagan and Buchanan 2016). Some, such as the Coalition for Evidence-Based Policy, even require the replication of

findings using a second RCT in a different implementation site to qualify for the 'Top Tier' category. Others, such as the Centre for Evidence-Based Crime Policy, are more flexible and include evaluations designated as 'moderately rigorous'. These less rigorous methodologies do not use RCTs but rely on carefully selected and controlled comparison groups. Based on evaluation data collected from third parties, program or policy outcomes are usually categorized as negative (ineffective or harmful), neutral (nsignificant, inconclusive, mixed results), or positive (promising, effective).

7. Only one third of monitoring platforms provide free access to the secondary data on which their assessment is based. Only 39% of surveillance platforms provide access to the full text of the legislative documents or scientific studies they analyze. The other platforms require users to be familiar with the use of legal databases or to have access to expensive academic online journals in order to review documentary materials.
8. More than half of monitoring tools offer download options at zero cost to access raw data: 61% of the monitoring tools analyzed in our sample enable users to download their datasets directly to perform new analyses, usually in Excel or CSV file formats; more rarely as SPSS files. All the platforms that provide this download functionality do it free of charge, although one (the Americans for Nonsmokers' Rights) offers to provide specialized data extraction services on a fee-for-service basis.

This summary review of a limited sample of policy monitoring platforms illustrates the practical challenges associated with the development of such tools in complex domains such as cybercrime prevention. Not all policy fields are mature enough to have access to well-established and well-funded program evaluation resources that can be leveraged to rate the effectiveness – or lack thereof – of policies. Cybercrime prevention is one of these; a policy monitoring platform in this domain would therefore need to adopt a more descriptive approach in the initial stages, as scientific evidence for the effectiveness of policies remains limited. In addition to international comparisons, one of its primary functions would be to highlight and outline policies and programs that require thorough evaluation before they can be promoted as successful strategies that deserve to be replicated.

Because cybercrime is a global problem addressed by local jurisdictions, the level of comparison should by definition cover local and national initiatives implemented in a broad range of countries. This would obviously have a significant impact on the resources needed to collect and analyze data required for this type of international comparative effort. For example, to capture policies and programs implemented in non-English speaking countries, which contain a majority of the world population and its internet users, people who can process official and scientific documents written in various languages must be recruited and trained. Clear selection and coding procedures that can be applied consistently by a significant number of collaborators must be designed, tested, and explained.

The multidisciplinary nature of cybercrime prevention policies, which often have legal, technical, and social implications, means that the information collected by a policy monitoring tool should also reflect these complementary dimensions. Such efforts are most likely to succeed if they involve researchers from a range of disciplines, such as criminology, computer science, psychology, law, political science, sociology, and economics, to name the most relevant ones. Given the ubiquity of technology in modern societies, cybercrime prevention policies cut across multiple policy domains that were once considered to belong to discrete spheres of activity, such

as crime prevention, national security, critical infrastructure protection, research and development, economic development, standardization, privacy protection, or education. As a result, efforts to monitor cybercrime prevention policies will require the mobilization of diverse forms of expertise.

4. Existing cybercrime prevention and cybersecurity policy monitoring tools

Several initiatives have already been created to consolidate information – objectives, level of maturity, and, to a lesser extent, outcomes – about cybercrime prevention and cybersecurity policies. A quick overview of these efforts and their main features is provided in this section in order to assess what has already been done and what knowledge gaps need to be filled. Although every effort has been made to include all known policy monitoring platforms in the cyber-domain, the dynamic nature of this area of research means that some recent initiatives may have been overlooked. The initiatives are discussed alphabetically.

The ***Cyber Readiness Index (CRI)***[3] was initially developed in 2013 by Melissa Hathaway (a former Bush and Obama administration official) for the Potomac Institute for Policy Studies (Hathaway 2013), and updated in 2015. The CRI examines the level of maturity that countries demonstrate in their efforts to develop cybersecurity capacities (Hathaway et al. 2015) and attempts to measure a country's operational capacities across seven dimensions: national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development (R&D), diplomacy and trade, and defense and crisis response. Each dimension is broken down into four components: statement (the existence of formal policies), organization (the existence of institutions that can implement those policies), resources (the allocation of financial and human resources as well as the establishment of measurement tools to assess the impact of cyber threats and the policies that address them), and implementation (evidence for the effectiveness of policies). Three levels of preparedness are used to assess each dimension: insufficient evidence (data is unavailable or inaccessible), partially operational (outputs are observed but their functionality remains difficult to measure), and fully operational (functioning activities can be observed and measured). It should be noted that the metrics used in this methodology focus more on the outputs of policies or how they are implemented than on their outcomes or what effects they produce. As of April 2019, the Cyber Readiness Team had released eleven in-depth country profiles for France, Germany, India, Italy, Japan, Morocco, the Netherlands, Saudi Arabia, South Africa, the United Kingdom, and the United States of America. Each country report can be downloaded as a PDF file but direct cross-country comparisons are not possible. Most of the data used in the country profiles is qualitative.

The ***Cybersecurity Capacity Portal***,[4] maintained by the Global Cyber Security Capacity Centre at the University of Oxford, provides general information about national and international capacity-building initiatives. It has developed a Cybersecurity Capacity Maturity Model for Nations (CMM) that assesses the capacities of countries across five dimensions[5]: policy and strategy; culture and society; education, training, and skills; legal and regulatory frameworks; and standards, organizations, and technologies. Each dimension includes sub-factors that seem

[3] http://www.potomacinstitute.org/academic-centers/cyber-readiness-index
[4] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front
[5] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition

exclusively qualitative and focus more on policy implementation and outputs than on outcomes. Each sub-factor is rated on a five-level scale (startup, formative, established, strategic, and dynamic). Of the 24 dimensions and sub-factors that make up the model, only one addresses the issue of cybercrime, folding investigation and prevention activities into a single component. The Portal website indicates that the CMM has been deployed in over 100 countries with financial support from the World Bank, the International Telecommunication Union, and other international organizations but only fourteen detailed country profiles (Albania, Bhutan, Cyprus, Iceland, Indonesia, Kosovo, Kyrgyzstan, Lithuania, Macedonia, Madagascar, Senegal, Sierra Leone, Uganda, and the U.K.) and a regional report providing a high-level analysis of 32 Latin American and Caribbean countries[6] are available for download.

The ***EU and Asia-Pacific Cybersecurity Dashboards*** are produced by The Software Alliance[7], a business group that represents the software industry. Their aim is to assess the maturity of cybersecurity policies for 28 European and 10 Asian countries. Each country is assessed on 25 criteria, mainly directed toward programs and activities grouped in five themes: legal foundations, operational entities, public-private partnerships, sector-specific cybersecurity plans, and education. Each criterion is rated as met, partially met, or absent. Data collection was carried out in 2015 and has not been updated since. There is no consolidated index or score and no ranking of countries. The downloadable PDF reports provide brief country profiles with additional qualitative information highlighting specific policies.

The ***GFCE Inventory*** (Global Forum on Cyber Expertise)[8], like the Cybersecurity Capacity Portal, is maintained by the Global Cyber Security Capacity Centre at the University of Oxford. It lists and describes international programs and initiatives by public and private stakeholders that seek to enhance cybersecurity and prevent cybercrime. The database is searchable by region (East Asia, Europe, North America, etc.) and theme (cybercrime, cybersecurity, data protection, e-governance). The descriptions of initiatives (usually a single sentence) contain summarized information about sponsor organizations, partners, targeted countries and groups, aims and objectives, types of activities undertaken, expected outcomes, time frames, and contact details. Little information is provided about the actual implementation and outcome of the listed initiatives. It is difficult to determine the number of initiatives listed in the Inventory, but as of April 2019, 45 vignettes were available in the cybercrime category. These vignettes cover a very diverse set of initiatives promoted by international organizations such as the UN, the Council of Europe, Interpol, and Europol, as well as capacity-building and training initiatives offered to developing nations by developed countries such as the U.S. and the U.K. as part of their international assistance programs.

The ***Global Cybersecurity Index*** is published by the International Telecommunications Union (ITU)[9]. The first version was released in 2014, with a second updated version published in 2017 and a third draft released in 2019. This database rates the cybersecurity capacities of 194 countries across five dimensions: legal measures, technical measures, organizational measures, capacity building, and cooperation, which are further broken down into 25 indicators. The ITU makes it very

[6] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

[7] http://cybersecurity.bsa.org/ and http://cybersecurity.bsa.org/2015/apac/

[8] https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce

[9] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

clear that the GCI measures the commitment of countries based on the actions they are taking rather than the impact their engagement has for users, such as increasing levels of protection. In the area of cybercrime, for example, the GCI's main concerns are the existence or absence of cybercrime legislation and law enforcement capacities. The effectiveness of the legislative framework and investigative or information-sharing initiatives are not measured. The GCI incorporates both primary data provided by countries themselves and publicly available secondary data. The weighting of the data produces a final country score that ranges from 0 to 1, with the U.K. the highest ranked country for 2018 with a score of 0.931 (ITU 2018), having replaced Singapore, whose score dropped from 0.925 to 0.898 in one year (ITU 2017a). More detailed country profiles were available for download on the ITU's website until the end of 2017 but have now been removed. An interactive tool allowing comparisons between countries remains online but without access to supporting data[10]. The data tables on which the final scores are calculated are not available for download.

The *International Cyber Developments Review (INCYDER) database* is maintained by the NATO Cooperative Cyber Defense Centre of Excellence[11]. It lists legal and policy documents adopted by seventeen international and regional organizations such as the UN, the OECD, the G7, the EU, etc. Because of its cyber defense focus, the INCYDER database contains very few cybercrime-related documents and does not include international police cooperation organizations such as Interpol or Europol in its coverage. The original documents are downloadable from the INCYDER platform and searchable by keyword, topic, and date. Background notes on the cybersecurity responsibilities of each international organization are also available. INCYDER does not address policy outcomes, nor does it include references to scientific publications that discuss and/or evaluate these policies.

The *National Cyber Security Index (NCSI)* was launched in 2016 by the Estonian e-Governance Academy[12], with support from the Estonian government and international private sector partners. This two-year, €200,000 project developed a methodology to measure countries' preparedness to prevent cyber threats, as well as their readiness to respond to cyber-attacks. The Index ranks 130 countries and is structured around 46 indicators arranged in three main categories (general cybersecurity, baseline cybersecurity, and incident and crisis management) and twelve capacities[13]. Points are assigned depending on the level of capacity achieved and an interactive tool allows between-country comparisons[14]. As in many other indexes, what gets measured is the existence of particular institutions and programs rather than their effectiveness—or lack thereof—in providing protection against cyber threats. The four indicators that deal specifically with cybercrime focus mainly on investigative capacities (the existence of a legislative framework, a dedicated cybercrime unit, a digital forensics unit, or a 24/7 contact point for international cybercrime) and ignore the prevention activities of public and private security organizations.

Although extremely valuable in providing frameworks that should enable governments to enhance their cybersecurity capacity and readiness, the methodologies, platforms, and indexes presented above also suffer from significant limitations. While the proliferation of reports

[10] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_GLO_Graphics.aspx
[11] https://ccdcoe.org/research/incyder/
[12] http://ncsi.ega.ee/
[13] https://ncsi.ega.ee/methodology/
[14] http://ncsi.ega.ee/ncsi-index/#

encourages broader conversations among stakeholders and increased production of relevant indicators and typologies, there is also a risk that overlap of effort will result in unhealthy competition and confusing results. A quick comparison of the top ten countries in the rankings published by the ITU's GCI and the e-Governance Academy's NCSI (shown in table 2) illustrates this point quite strikingly. Although the ITU and e-Governance Academy use very similar indicators, they agree on only half of the top ten performers – the Czech Republic, which comes first in the NCSI ranking, is 71st in the GCI, while the UK and the US, which rank as first and second in the GCI only appear in 14th and 29th position in the NCSI ranking. These major discrepancies derive from the data collection process: the quality of information available remains uneven from one country to another and becomes subject to interpretation by rating teams when they have to assign a score to a particular institutional setup with which they may not be very familiar. For example, the main reason why the US is ranked so poorly by the NCSI is that it received 0 point for the existence of a cyber threats analysis unit, 0 point for the publication of an annual public cyber threat report, 0 point for the existence of a competent supervisory authority for digital services, does not have a government-led e-identification scheme, and received 0 point on the protection of personal data criteria. By contrast, the Czech Republic received top scores on each of these dimensions from NCSI, despite a much tougher assessment by the GCI team. Biases are inevitably introduced when complex whole-of-government policies are reduced to easily-digestible metrics, despite the raters' best intentions, but they remain highly problematic when they generate such variance in ranking outcomes for certain countries. A similar lack of consistency has also been noted for crime prevention registries and illustrates the challenge of trying to rate the effectiveness of a policy or a country performance (Fagan and Buchanan 2016: 21).

INSERT TABLE 2 ABOUT HERE

The platforms reviewed above use countries as their unit of analysis to produce aggregate scores or assessments. This approach supports global policy transfers but prevents researchers and decision makers from examining the individual benefits or failures of specific policies and programs. As a result of this broad country-focused approach, and also because there is a paucity of quantitative data available on cybersecurity capacities and their effects, all of the monitoring platforms rely on qualitative data sourced from official and legal documents: the metrics produced by these initiatives are derived from the accumulation of publicly available information on the existence or absence of a limited set of institutions, programs, and practices. This explains to a large extent why, despite claims of evidence-based methodologies, most platforms focus more on the implementation of policies and their outputs – such as the development of emergency response teams, legal information sharing frameworks, public-private partnerships, or awareness programs – and less on the outcomes of those policies, which would require hard metrics such as investments made, infection rates recorded, or number of users protected from various harms. There is mounting evidence that there is a direct relationship between increased capacities and enhanced cybersecurity (Dutton et al. 2017), but a more granular understanding of which policies deliver what benefits and how they achieve these results remains elusive.

Cybercrime remains a secondary concern for many of the cybersecurity policy monitoring initiatives reviewed in this article. This probably reflects the lack of resources allocated to police services to deal with cybercrime compared to the impressive investments made by governments

to enhance the cyber-capacities of their armed forces and intelligence agencies, or the economic development investments made by public and private entities in order to join a thriving private cybersecurity market. The fact that criminologists are underrepresented in the growing field of cybersecurity studies and have received limited research funding to conduct empirical and evaluative research may also explain why cybercrime prevention policies remain an afterthought in the scientific literature, with a few notable exceptions (Holt and Bossler 2016, Button and Cross 2017, Maimon and Louderback 2019).

Finally, there are two additional limitations associated with the recency and availability of data on these platforms. First, very few indexes and platforms regularly update the data they collect. While this reflects the resource-intensive and time-consuming nature of such undertakings, it makes it difficult to map a country's progress or change in policies. Second, the final products are released as 'static' PDF documents, which in several cases are complemented by interactive visualization tools. However, none of the cybersecurity initiatives reviewed here makes its databases available to third party researchers in a readily processable format (such as Excel files, for example).

5. The case for a cybercrime prevention surveillance platform

In light of the extensive policy surveillance knowledge that has been developed in domains such as public health, education, violence prevention, and environment protection, and considering how widespread cybercrime has become in contemporary societies, the creation of a cybercrime prevention surveillance tool that would complement the more general initiatives discussed above should be a priority. Such a platform could systematically collect detailed information about individual cybercrime prevention policies in a format that would facilitate their cataloguing, retrieval, analysis, and evaluation. This data should be updated regularly and accessible to independent researchers and policy makers, which would generate new insights on the effectiveness of existing policies, as well as their unintended or counterproductive effects.

A pilot study for such a platform was conducted at the Université de Montréal's International Centre of Comparative Criminology during the first half of 2017 with financial support from the Korean Institute of Criminology. The study was aimed at leveraging insights from existing policy surveillance tools to design a data-capture framework that incorporated the most relevant information about cybercrime prevention policies and then testing this framework on a small sample of policies to determine the feasibility and scalability of the approach. Table 3 gives an overview of the coding framework developed during the pilot.

INSERT TABLE 3 ABOUT HERE

The coding framework introduced above could be used to support an online cybercrime prevention monitoring platform with simple search functionalities. For example, a country or a local community planning to design a new cybercrime prevention program to combat online fraud or to prevent cyberbullying could examine the programs that already exist by searching the platform using relevant keywords ("anti-phishing campaigns" or "cyber-bullying programs"), but also by scanning the fields that describe the different targeted issues or undesirable situations. In the case of cyber-bullying, additional searches could also be performed to include other prevention programs that target the same population (youth) in order to identify various strategies

that have been imagined to reach this particular group more effectively and with more credibilty. Alternative searches might also help policy designers extract inspiring ideas to expand their range of funding sources, implementation partners or incentivization strategies. Finally, search filters could also be used to quickly identify the implementation hurdles that similar programs have had to overcome and the solutions they came up with. The coding scheme presented here would also allow policy makers to quickly identify programs for which robust evaluations exist and to be exposed to a diversity of evaluative methodologies that they could borrow from. By providing additional references (both from the professional and scientific literatures), such a platform would also act as a online library on cybercrime prevention.

New summaries would be added regularly. Specific types of interventions or countries could be prioritized to focus on policy innovation clusters or to test the effectiveness of promising strategies. Designing, implementing, and maintaining such a platform is an ambitious goal that will require development of a large-scale international collaboration network of researchers, policy-makers, and volunteers. Ideally, contributors to the database would need to master the local languages in which cybercrime prevention policies are drafted, implemented, and evaluated to avoid over-reliance on English-language documents. Particular efforts should also be made to involve academics from the developing world, as more than four billion people have access to the internet through a mobile broadband connection and are therefore exposed to a broad range of online criminal harms that need to be addressed through a diverse set of prevention approaches (ITU 2017b). Despite these hurdles, I am convinced that creating such a cybercrime prevention monitoring platform and making its data publicly available and easily searchable would greatly advance our collective capacity to respond to online criminal harms.

Conclusion

Governments around the world use the labels “cybercrime” and “cybersecurity” to deliver a broad range of interventions designed to prevent and mitigate a diverse portfolio of online criminal harms. These interventions vary greatly in terms of goals, implementation, delivery strategies, levels of coerciveness, types of engagement with the private sector, and outcomes. However, most of them are similar in the unfortunate scarcity of empirical evaluations that could help policy-makers and citizens assess which policies are producing the expected results and which are underperforming or should be abandoned outright. This lack of evidence is surprising considering the technical nature of cybersecurity and the ease with which performance indicators and metrics can be collected using automated methods. Given the considerable investments being made by governments and organisations to improve cybersecurity, it is concerning that there are not more scientifically rigorous efforts being undertaken to establish which policies and programs are delivering measurable improvements to the safety of our digital ecosystem. In the limited sample of surveillance tools used in the pilot study discussed above, fewer than one third of the reviewed policies had been evaluated and even fewer had been assessed independently.

The tools and platforms associated with the policy monitoring approach facilitate knowledge transfers, cross-jurisdictional comparisons, and evidence-based interventions. I have outlined the main features of a diversified sample of existing policy monitoring tools and shown how they could be applied to the field of cybercrime prevention, including the specific challenges that would need to be met. It is now up to cyber-criminologists to determine the relevance of this framework, its feasibility, and the collaborative resources that would be needed to translate it into reality.

Acknowledgements

The author would like to thank the participants to the First Annual Conference on the Human Factor in Cybercrime, as well as the anonymous evaluators and the editors of this special issue (Dr. Adam Bossler and Dr. Tamar Beremblum) for their invaluable feedback on earlier versions of this manuscript. This research was funded by the Korean Institute of Criminology, with stellar research assistante provided by Elsa Euvrard, Marilyne Bernier, Chloé Majdalany, Shannon McPhail, and Yuan Stevens.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., and S. Savage. 2013. "Measuring the Cost of Cybercrime." In *The Economics of Information Security and Privacy*, edited by R. Böhme. 265-300. New York: Springer.

Bilodeau, H., Lari, M., and M. Uhrbach. 2019. *Cyber Security and Cybercrime Challenges of Canadian Businesses, 2017*. Ottawa: Statistics Canada.

Bothwell, L., Greene, J., Podolsky, S., and D. Jones. 2016. "Assessing the Gold Standard – Lessons from the History of RCTs." *The New England Journal of Medicine* 374 (22): 2175-2181.

Burris, S., Wagenaar, A., Swanson, J., Ibrahim, J., Wood, J., and M. Mello. 2010. "Making the Case for Laws that Improve Health: A Framework for Public Health Law Research." *Milbank Quarterly* 88 (2): 169-210.

Burris, S., Hitchcock, L., Ibrahim, J., Penn, M., and T. Ramanathan. 2016. "Policy Surveillance: A Vital Public Health Practice Comes of Age." *Journal of Health Politics, Policy and Law* 41 (6): 1061-1083.

Button, M., and C. Cross. 2017. *Cyber Frauds, Scams and their Victims*. New York: Routledge.

Chriqui, J., O'Connor, J., and F. Chaloupka. 2011. "What Gets Measured, Gets Changed: Evaluating Law and Policy for Maximum Impact." *The Journal of Law, Medicine & Ethics* 39 (1): 21-26.

Cross, C. 2016. "Using Financial Intelligence to Target Online Fraud Victimisation: Applying a Tertiary Prevention Initiative." *Criminal Justice Studies* 29 (2): 125-142.

CSE. 2017. *Cyber Threats to Canada's Democratic Process*. Ottawa: Communications Security Establishment.

CSIS. 2014. *Net Losses: Estimating the Global Cost of Cybercrime*. Washington, DC: Center for Strategic and International Studies.

Cybersecurity Ventures. 2017. *Cybersecurity Market Report*. Menlo Park. Accessed 15 August 2019. https://cybersecurityventures.com/cybersecurity-market-report/.

Duckett, C. 2016. "Budget 2016: Australian Cyber Strategy Implementation Broken Out." *ZDNet*. Accessed 15 August 2019. http://www.zdnet.com/article/budget-2016-australian-cyber-strategy-implementation-broken-out/.

Dupont, B. 2017. "Bots, Cops and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." *Crime, Law and Social Change* 67 (1): 97-116.

Dutton, W. H., Creese, S., Shillair, R., Bada, M., and T. Roberts. 2017. *Cyber Security Capacity: Does it Matter?* Accessed 15 August 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938078.

European Commission. 2016. *Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tackle Cyber-Threats*. Accessed 15 August 2019. http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

Fagan, A., and M. Buchanan. 2016. "What Works in Crime Prevention? Comparison and Critical Review of Three Crime Prevention Registries. *Criminology & Public Policy* 15 (3): 1-33.

Florêncio, D., and C. Herley. 2013. "Sex, Lies and Cyber-Crime Surveys." In *Economics of Information Security and Privacy III*. Edited by B. Schneier, 35-53. New York: Springer.

Furnell, S., Emm, D., and M. Papadaki. 2015. "The challenge of Measuring Cyber-Dependent Crimes." *Computer Fraud & Security* 10: 5-12.

Gandel, S. 2015. "Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year." *Fortune*. Accessed 15 August 2019. http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

Gartner. 2017. *Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017*. Accessed 15 August 2019. http://www.gartner.com/newsroom/id/3784965.

Hathaway, M. 2013. *Cyber Readiness Index 1.0*. Accessed 15 August 2019. http://www.belfercenter.org/sites/default/files/legacy/files/cyber-readiness-index-1point0.pdf.

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., and F. Spidalieri. 2015. *Cyber Readiness Index 2.0 - A Plan for Cyber Readiness: A Baseline and an Index*. Washington DC: Potomac Institute for Policy Studies.

Holt, T., and A. Bossler. 2016. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. New-York: Routledge.

Hutchings, A., and T. Holt. 2017. "The Online Stolen Data Market: Disruption and Intervention Approaches." *Global Crime* 18 (1): 11-30.

ITU. 2017a. *Global Cybersecurity Index (GCI) 2017*. Geneva: International Telecommunication Union.

ITU. 2017b. *Measuring the Information Society Report 2017*. Geneva: International Telecommunication Union.

ITU. 2018. *Global Cybersecurity Index 2018*. Geneva: International Telecommunication Union.

Lee, R. M., and T. Rid. 2014. "OMG Cyber!" *The RUSI Journal* 159 (5): 4-12.

Levi, M. 2017. "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues." *Crime, Law and Social Change* 67 (1), 3-20.

Maimon, D., Alper, M., Sobesto, B., and M. Cukier. 2014. "Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System." *Criminology* 52 (1): 33-59.

Maimon, D., and E. Louderback. 2019. "Cyber-Dependent Crimes: An Interdisciplinary Review." *Annual Review of Criminology* 2: 191-216.

Osborne, G. 2015. *Chancellor's Speech to GCHQ on Cyber Security*. Accessed 15 August 2019. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

Presley, D., Reinstein, T., and S. Burris. 2015. *Resources for Policy Surveillance: A Report Prepared for the Centres for Disease Control and Prevention Public Health Law Program*. Accessed 15 August 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567695.

Reep-van den Bergh, C., and M. Junger. 2018. "Victims of Cybercrime in Europe: A Review of Victim Surveys." *Crime Science* 7 (5): 1-15.

Sampson, R. J. 2010. “Gold Standard Myths: Observations on the Experimental Turn in Quantitative Criminology.” *Journal of Quantitative Criminology* 26 (4): 489-500.

Sherman, L., Gottfredson, D., MacKenzie, D., Eck, J., Reuter, P., and S. Bushway. 1997. *Preventing Crime: What Works, What Doesn’t, What’s Promising*. Washington, DC: U.S. Department of Justice.

The White House. 2019. *Cybersecurity Funding*. Accessed 15 August 2019. https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf.

WEF. 2017. *The Global Risks Report 2017: 12th edition*. Geneva: World Economic Forum.

Zurich. 2014. *Risk Nexus - Beyond Data Breaches: Global Interconnections of Cyber Risk*. Zurich: Zurich Insurance Company.

Table 1. A Sample of Policy Surveillance Platforms Accessible Online (listed alphabetically)

Platform	Policy domain	Data collected and URL
Alcohol Policy Information System (APIS)	Public Health	Provides detailed information on a wide variety of alcohol-related policies in the United States at both state and federal levels. Detailed state-by-state information is available for 35 alcohol-related policies. The website now has information on recreational cannabis. http://alcoholpolicy.niaaa.nih.gov/
Americans for Nonsmokers' Rights (ANR)	Public Health	The American Nonsmokers' Rights Foundation U.S. Tobacco Control Laws Database has tracked, collected, and analyzed tobacco control ordinances, by-laws, and Board of Health regulations since the early 1980s. http://www.no-smoke.org/
Blueprints for Healthy Youth Development list	Youth Development	Blueprints focuses on youth programs to prevent violence, delinquency, drug use and promote mental and physical health, self-regulation, and educational achievement outcomes. http://blueprintsprograms.com/
Center for Evidence- Based Crime Policy	Criminal Justice	The Evidence-Based Policing Matrix is a visualization tool that is mainly a meta-analysis of police interventions. It evaluates and lists all research studies on police interventions and classifies them across 3 axis: - Focus; - Reactiveness; - Scope of target. http://cebcp.org/evidence-based-policing/the-matrix/
Child Trends	Public Health	The Child Trends Data Bank includes regularly updated data on more than 125 indicators of the well-being of children and youth, with clear summaries of the underlying research, explanation of important trends, and downloadable tables and graphs. http://www.childtrends.org/
Chronic Disease State Policy Tracking System	Public Health	The Chronic Disease State Policy Tracking System is designed to provide detailed policy information to facilitate research and share how U.S. states are addressing chronic health issues. https://nccd.cdc.gov/CDPHPPolicySearch/default.aspx
Classification of Laws Associated with School Students (CLASS)	Public Health	The CLASS website uses two policy classification systems to score state-level codified laws for physical education (PE) and nutrition in schools. Differences in codified state laws in nutrition and physical education across states are assessed over time. http://class.cancer.gov/
Coalition for Evidence-based Policy	Cross-sectoral	The Coalition for Evidence-Based Policy listed and summarized programs that showed credible evidence of important effects on people's lives in the fields of prenatal and early childhood care, K-12 education, teen pregnancy prevention, crime prevention, homelessness, employment and welfare, obesity and disease prevention, mental health, international development, etc. It wound down its operations in the spring of 2015; the Coalition's leadership and core elements of the group's work have been integrated into the Laura and John Arnold Foundation. The policy surveillance platform remains accessible online. http://coalition4evidence.org/
Crime Solutions Database - Office of Justice Programs	Criminal Justice	CrimeSolutions.gov is a database that contains information on justice-related programs that had been rigorously evaluated. https://www.crimesolutions.gov/
Global Policing Database (GPD)	Criminal Justice	The Global Policing Database (GPD) is a web-based and searchable database designed to capture all published and unpublished experimental and quasi-experimental evaluations of policing interventions conducted since 1950.

		http://www.gpd.uq.edu.au/search.php
Guttmacher Institute	Public Health	The Guttmacher Institute provides information on key sexual and reproductive health policies in the United States and globally. https://data.guttmacher.org/regions
LawAtlas	Public Health	LawAtlas includes policy surveillance on a broad set of state laws including those pertaining to distracted driving, medical marijuana, access to naloxone, Good Samaritan overdose laws, water quality, and more. http://lawatlas.org/
Law Center to Prevent Gun Violence	Public Health	The Law Center to Prevent Gun Violence website covers over 35 domains related to gun laws (minimum age to purchase, universal background checks, assault weapons, imitation and toy guns, firearm registration, etc.). http://smartgunlaws.org/search-gun-law-by-gun-policy/ http://gunlawscorecard.org/
National Registry of Evidence-based Programs and Practices (NREPP) - SAMHSA	Public Health	The National Registry of Evidence-based Programs and Practices provides information on substance abuse and mental health interventions. http://nrepp.samhsa.gov/01_landing.aspx
State Legislated Actions on Tobacco Issues (SLATI)	Public Health	SLATI tracks state tobacco control laws, such as restrictions on smoking in public places and workplaces and tobacco taxes, on an ongoing basis. http://www.lungusa2.org/slati/
State School Health Policy Database	Public Health	The State School Health Policy Database tracks policies related to school nutrition by topic area. http://www.nasbe.org/healthy_schools/hs/bytopics.php
State Tobacco Activities Tracking & Evaluation System (STATE)	Public Health	The State Tobacco Activities Tracking & Evaluation System is an interactive application that presents current and historical state-level data on tobacco use prevention and controls. https://www.cdc.gov/statesystem/
Stop Bullying	Criminal Justice	Stop Bullying lists policies and laws related to bullying, cyberbullying, and related behaviors. https://www.stopbullying.gov/laws/index.html#listing

Table 2. Comparison of Top Ten Performers in GCI and NCSI Indices

Rank	GCI 2018	NCSI 2019
1.	United Kingdom	Czech Republic
2.	United States	Estonia
3.	France	Spain
4.	Lithuania	Lithuania
5.	Estonia	Greece
6.	Singapore	France
7.	Spain	Finland
8.	Malaysia	Denmark
9.	Norway	Netherlands
10.	Canada	Germany

Table 3. Structure of the Coding Framework

Categories	Data Fields
Overview of the policy and search filters	Summary
	Nature of the policy
	Related policies and legislation
	Keywords
	Snapshot data
Description of the policy	Date of implementation or launch
	Place of implementation
	Geographical scope
	Instigator of the policy
	Targeted issue or situation
	Targeted population
	Goals of the policy
	Components of the policy
	Agents in charge of implementation
	Costs
	Source of funding
	Penalties
	Incentives
	Challenges
	Implementation information
Evaluation of the policy	Existence of an evaluation
	Evaluation type
	Evaluator
	Methodology
	Outcomes
Additional references	URL
	Peer-reviewed publications
	Media articles
	Official documents