Design Framework for the Creation of a Cybersecurity Policy Observatory

Canada Research Chair in
Cybersecurity International Centre
for Comparative Criminology –
Université de Montréal

A report for the Korean Institute of Criminology
December, 2017

KIC Korean institute of Criminology

CICC Centre international de criminologie comparée

Design Framework for the Creation of a Cybersecurity Policy Observatory

Canada Research Chair in Cybersecurity
International Centre for Comparative Criminology – Université de Montréal

By Dr. Benoît Dupont, Elsa Euvrard, Chloé Majdalany, Shannon McPhail, and Michael Joyce

A report for the Korean Institute of Criminology

December, 2017

KIC Korean Institute of Criminology

CICC Centre international de criminologie comparée

International Centre for Comparative Criminology – Université de Montréal

Université de Montréal, Montreal, Canada

URL- http://www.cicc.umontreal.ca/en

Director

Benoît Dupont

Researchers

Elsa Euvrard

Chloé Majdalany

Shannon McPhail

Michael Joyce

Table of Contents

Tables and Figures

Tables

Figures

Preface

As governments, businesses and individuals start to grasp the pivotal role cybersecurity plays in our daily lives and understand the new digital risk landscape created by billions of connected devices, new knowledge is needed to assess what policies and approaches will be required to help citizens and communities stay safe online.

Despite the billions of dollars invested by governments and multinationals to enhance their online security posture, the limitations of a technological approach have become clear. In other words, cybersecurity and the prevention of cybercrime are now more than just technological problems. They have become social and policy problems that must be addressed through a broad set of intervention strategies and tools.

This report attempts to outline our knowledge needs in this area of vital importance for our digital societies. It makes a case for a more systematic cybersecurity policy monitoring platform, inspired by similar approaches in fields as diverse as public health, youth development and criminal justice. The purpose of policy monitoring is to systematically collect, analyse and disseminate information about policies implemented in various settings to better understand which ones are effective, efficient and those that do not deliver any outcome, or worse, produce adverse effects. This report highlights lessons drawn from an extensive review of existing policy surveillance platforms in order to lay out the principles that should guide the creation of a Cybersecurity Policy Observatory. We also provide an overview of existing cybersecurity monitoring tools, in order to avoid the unnecessary duplication of resources. Finally, we provide a sample of high profile cybersecurity policy summaries; to clearly illustrate the type of data such an observatory would make available to its users.

The benefits of this observatory are realisable at the global scale. Accordingly, the exercise must be truly international and go beyond the usual focus on English speaking countries to include all nations that are developing creative cybersecurity governance and regulatory approaches to combat cybercrime and foster innovation and economic prosperity.

In that sense, the collaboration between the Korean Institute of Criminology and the International Centre for Comparative Criminology that made this project possible is exemplary. A memorandum of understanding was signed between the two institutions in August 2014 to foster joint research projects and academic exchanges. The extensive networks both centres have built and sustained over the years in Asia, North America, Europe, Africa and Latin America place them in a unique position to deliver a truly global perspective on what will prove to be one of humanity's most complex challenges.

1 Introduction

The numbers and statistics available on cybersecurity risks and investments, however imprecise and fragmentary, are staggering. In 2014, the Center for Strategic and International Studies estimated that cybercrime and espionage costs $445 billion annually in a report sponsored by the security firm McAfee, which would roughly amount to 1% of global income (CSIS 2014). The insurance company Lloyd's arrived at the same number in 2015 ($400 billion a year) when it tried to measure 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 UK data suggests that the global cost of cybercrime around the 2010s could reach $75 billion—and $225 billion if traditional crimes transitioning to cyber were included (Anderson et al. 2013). As a result, government and business leaders have ranked cyber-risks at the top of their security concerns for the past few years, and are anticipating even more disruptive outcomes as our societies become more cyber-dependent and interconnected than ever (WEF 2017, Zurich 2014).

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 (Cybersecurity Ventures 2017). The same consultancy predicts sustained growth rates of 12-15% until 2021. Gartner (2017), another widely-cited consultancy, produced a more conservative assessment with a worldwide spending estimate of $86.4 billion for 2017 and 7% annual growth. Both these numbers are impressive in the current economic context where slow growth has become the norm for Western economies. Beyond the expected threats against critical infrastructures and online financial services, recent events in the U.S., France, and approximately 40 other nations have also highlighted how cyber threats can also target electoral processes and undermine the trust citizens have placed in their 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 from their defense and R&D budgets to implement new programs that will enhance their capacities to address cyber risks. For example, the U.S. federal government spent $14 billion for cybersecurity across various agencies in 2016 (The White House 2016), with a request for a 35% increase by President Obama for the 2017 fiscal year. In the U.K., the Chancellor unveiled cybersecurity investments of £1.9 billion over five years in November 2015, which complemented existing information security spending to bring the overall government's commitment to £3.2 billion for cybersecurity (Osborne 2015). Australia, a middle power, has also announced in 2016 a comprehensive cybersecurity strategy that will be

allocated 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 than that in matching funds (European Commission 2016).

1.1. Why we need to more systematically track cybersecurity policies

The above numbers only reflect a fraction of the significant budgets allocated by governments, international organizations and businesses across the world to address the complex problems created by cyber risks. Unfortunately, there is no source of consolidated data that would enable us to measure and track these efforts at the global and national levels, nor do we have a centralized database of the various policies and programs implemented by public, private and community stakeholders to manage those risks. This lack of information, in a budgetary context where billions of dollars are spent on cybersecurity and where these numbers will grow at a steady pace for the next few years, is problematic for three main reasons.

1. It prevents us from being able to systematically assess the nature, effectiveness and efficiency of the various policies that are being adopted across the world. In other words, the lack of a common framework tracking cybersecurity policies, their features and innovations, which would be a first step towards a more rigorous measurement of their impact (i.e. whether they achieve their objectives at a reasonable cost) or the lack thereof, severely limits the evidence base of which approaches works and which do not. Making important decisions on such flimsy evidence creates avoidable risk.

2. At the international level, this lack of baseline information restricts the dissemination of knowledge and impedes the adoption of policies that have been proven to deliver positive outcomes, as well as preventing the debunking of failed or counterproductive policies. Lessons learned locally are not shared globally, although cybersecurity problems are very similar across countries at various stages of technological development.

3. Beyond the lack of evaluation and sharing, the absence of a common framework to analyze cybersecurity policies also hinders coordination efforts that would deliver more effective responses to transnational cybercrime and cyber-risks. International organizations such as the International Telecommunications Union, 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 on which policies are already being implemented by which

countries at what cost and for what results reduces the opportunities for policy harmonization and synchronization.

Cybersecurity is certainly not the first policy domain to face the problem of a lack of the information integration needed to facilitate the implementation of effective or promising policies and intervention strategies in diverse local and national contexts. Complex domains such as public health, education, environmental protection, urban planning or 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.

1.2. Policy surveillance: definition and principles

Policy surveillance has been defined as "the systematic collection, analysis and dissemination of information about laws and other policies" (Chriqui et al. 2011: 21; Presley et al. 2015: 53). Its main objective is to know "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). These methodologies differ from more classical policy analysis by their scientific ambition: rigorous protocols are designed to support the monitoring process and specify the laws and policies of interest, inclusion and exclusion criteria are outlined, search methodologies and their limits are acknowledged, and quantitative and qualitative coding schemes are designed to minimize analyst subjectivity (Burris et al. 2010: 182). Policy surveillance adopts a dynamic approach through regular updates to the data. By tracking the progress of policies at specific reference dates or intervals it makes possible subsequent longitudinal analyses of outcomes and impacts (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 can 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 to foster research projects that evaluate important policies at reduced costs. They also seek to make it simpler for policy-makers and end-users to understand the large number of policies that are relevant to their area of interest, as well as their key sub-components, and as a result to develop 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, such as is the case in cybersecurity (Lee and Rid

2014).

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

1. Significance of the problem targeted by the policy (focuses policy surveillance on pressing issues);
2. Policy salience (reflects the aggregate interest in a policy by a broad range of stakeholders);
3. Existence of evidence or evaluation (policy surveillance enables policy evaluation, and as a result, new policies that are widely adopted but have not yet been evaluated are prioritized);
4. Whether the policy is an identified national priority (allows policy surveillance to better track how national strategies are actually implemented and translated into measurable programs);
5. Cost of conducting the policy surveillance (policies vary greatly in terms of information accessibility and complexity, which generates significant costs that must be considered at the selection stage).

1.3. Preliminary review of existing policy surveillance platforms

In order to better understand how policy surveillance platforms are developed and maintained in practice, our team conducted an extensive literature review on the subject that identified eighteen platforms and examined in detail the structure of their data and how it was made available online. This sample is by no means comprehensive, as Presley et al. (2015: 41-51) list more than 160 U.S. surveillance resources following policies in domains as diverse as tobacco control, school nutrition, anti-bullying, immigration, and climate change; among others. Burris et al. (2016: 1071) provide a few more examples of policy surveillance tools supported by international organizations such as the International Labor Organization, the World Health Organization, and the Campbell Collaboration, which is an international clearinghouse that promotes evidence-based policies and practices and lists more than two dozen evidence portals that perform policy monitoring functions[1].

Our sample is described in Table 1 below. Each of the listed platforms was reviewed to best capture their key features and to identify best practices that could be transferred to a cybersecurity policy surveillance initiative.

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

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 info 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, 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 list all research studies on police interventions and classify them across 3 axes: - Focus; - Reactiveness; - Scope of target. http://cebcp.org/evidence-based-policing/the-matrix/
Child Trends	Public Health	The Child Trends DataBank 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. Assess differences in codified state laws in nutrition and physical education across states over time. http://class.cancer.gov/

Platform	Policy Domain	Data Collected and URL
Coalition 4 Evidence	Cross-sectoral	The Coalition for Evidence-Based Policy listed and summarized programs with 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, and 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 were 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 Center for Population Research Innovation and Dissemination	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 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

Platform	Policy Domain	Data Collected and URL
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

Ten dimensions of the policy surveillance programs were examined:

- Policy domain: policy surveillance seems to be considerably more developed in public health, which accounts for a vast majority of platforms (72%), followed by crime and justice (17%), youth development (6%) and a cross-sectoral initiative (6%);

- Leadership: 50% of the efforts examined in our sample are led by public sector agencies, 39% by non-profits and NGOs (mainly academic institutions and non-profit foundations), with a remaining 11% reflecting joint efforts by these two groups;

- Comparison type: more than half of this very U.S. centric sample compares legislation, policies and programs across American municipalities and states (56%), while only one platform provides international comparative data (6%). 39% of the reviewed databases describe policies as isolated initiatives, and only two platforms (crimesolutions.gov and coalition4evidence.org) are able to provide multiple evaluation results that can be compared and averaged out for each selected program. Finally, 28% of the platforms track and compare policies and legislation over time;

- Data aggregation: 100% of the databases aggregate data and information produced by third parties, such as program implementation agencies, official statistical sources or independent evaluators. The costs of collecting data directly or conducting their own evaluations appear to be prohibitive;

- Literature review: As a direct consequence of the aggregation approach highlighted above, all platforms (100%) rely on literature reviews to describe and evaluate the policies and programs they include in their databases. The depth of these literature reviews varies greatly: while certain platforms provide long lists of references for every program, others prefer to only cite one or two studies that provide the more detailed description or evaluation of a policy or program's outcomes;

- Evaluation: Not all monitoring platforms provide evaluation outcomes for the policies they list. In fact, only slightly more than half of our sample (56%) were seen to do so. The remaining 44% focus instead on the comprehensive description of local legislative frameworks, in the hope that this formatted data will be useful to potential independent evaluators. Most platforms rating the effectiveness of policies use the gold standard of Randomized Control Trials (RCTs) as their main criteria. 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 bit more

flexible and include evaluations that are defined as “moderately rigorous”. These less rigorous methodologies would not use RCTs, but would still rely on separate comparison groups that would be carefully selected and controlled for. Based on the evaluation data collected from third parties, the outcomes are usually categorized as negative (ineffective or harmful), neutral (non-significant, inconclusive, mixed results) or positive (promising, effective);

- Data availability: Only approximately one third (39%) of surveillance platforms provide access to the full text of the legislative and policy documents they analyze. This means that the other platforms require users to be familiar with the use of legal databases and have access to expensive academic online journals to work with the primary materials;

- Download option and costs: 61% of the monitoring platforms 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 on a fee-for-service basis.

1.4. Lessons for a cybersecurity policy monitoring platform

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 cybersecurity. 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 policies’ effectiveness; or the lack thereof. Cybersecurity is one of them, and a policy monitoring platform in this domain would therefore need to adopt a more descriptive approach in the initial stages, as the scientific evidence of policies’ effectiveness remains limited. Beyond international comparisons, one of its primary functions will therefore be to highlight and outline policies and programs requiring thorough evaluations before they can be promoted as successful.

Because cybersecurity is a global problem addressed by local jurisdictions, the level of comparison will by definition need to cover local and national initiatives implemented across the world, which has a significant impact on the resources needed to collect and analyze the available data. To capture policies implemented in non-English speaking countries, which represent a majority of the world population and internet users, people who can process official and scientific documents written in various languages must be recruited. Clear selection and coding procedures that can be applied consistently by a significant number of collaborators must also be designed, tested and explained.

The cross-sectoral nature of cybersecurity 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. It implies that such efforts are most likely to succeed if they involve researchers from a range of disciplines, including computer scientists, criminologists, legal scholars, political scientists, sociologists, etc. The ubiquity of technology in modern societies also implies that cybersecurity policies cut across a broad range of policy domains that were once considered as belonging to discrete spheres of activity, such as national security, critical infrastructure protection, crime prevention, R&D, economic development, standardization, privacy protection or education. As a result, efforts to monitor cybersecurity policies will require the mobilization of diverse forms of expertise.

1.5. Existing cybersecurity policy monitoring tools

Several initiatives have already started to consolidate information about cybersecurity policies, their objectives, their level of maturity, and to a lesser extend their outcomes. In order to avoid the unnecessary duplication of resources, a quick overview of these efforts and their main features is provided below. The list is not exhaustive and we invite initiatives we may have overlooked to contact us so that we can include them in future publications. The initiatives are listed alphabetically.

Cyber Readiness Index (Potomac Institute for Policy Studies)[2]

Initially developed by Melissa Hathaway (a former Bush and Obama administration official) in 2013 (Hathaway 2013), then updated in 2015, the Cyber Readiness Index (CRI) examines the level of maturity that countries demonstrate in their efforts to develop cybersecurity capacities (Hathaway et al. 2015). The CRI seeks 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 five 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 of policies' effectiveness). Three levels of readiness are used to assess each dimension: insufficient evidence (when data is unavailable or inaccessible), partially operational (outputs are observed but their functionality remains difficult to measure), and fully operational (functioning

[2] http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

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 rather than on their outcomes or what effects they produce). As of September 2017, the Cyber Readiness Team had released eight in-depth country profiles for the United States of America, France, Japan, Germany, the United Kingdom, the Netherlands, India and Italy. Each country report can be downloaded as a PDF file and some of them are available translated into Russian, but direct cross-country comparisons are not possible. Most of the data used in the country profiles is qualitative.

Cybersecurity Capacity Portal (Global Cyber Security Capacity Centre – University of Oxford)[3]

The Cybersecurity Capacity Portal provides general information about national and international capacity building initiatives. It has developed a Cybersecurity Capacity Maturity Model for Nations (CMM) that assesses countries' capacities across five dimensions[4]: 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 exclusively qualitative and that 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). The portal website indicates that the CMM has been deployed in over 40 countries, but only six detailed country profiles (the UK, Kosovo, Bhutan, Uganda, Senegal and Indonesia) and a regional report providing a high-level analysis of 32 Latin American and Caribbean countries[5] are available for download.

EU and Asia-Pacific Cybersecurity Dashboards (BSA The Software Alliance)[6]

These two reports produced by a business group representing the software industry's aim 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 that are grouped in five themes: legal foundations, operational entities, public-private partnerships, sector specific cybersecurity plans, and education. Each criterion is either met, partially met or absent. The 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 either. The downloadable PDF reports provide brief country profiles with additional qualitative information highlighting specific policies.

---

[3] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front

[4] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition

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

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

GFCE Inventory (Global Forum on Cyber Expertise and Global Cyber Security Capacity Portal)[7]

Published on the same website as the Cybersecurity Capacity Portal, the GFCE Inventory lists and describes programs and initiatives implemented by public and private stakeholders that seek to enhance cybersecurity. The database is searchable by region (East Asia, Europe, North America, etc.) and theme (cybercrime, cybersecurity, data protection, e-governance). The initiatives' descriptions contain summary information (usually in a single sentence) about sponsor organizations, partners, targeted countries and groups, aims and objectives, types of activities undertaken, expected outcomes, timeframes, and contact details. Little information is provided on the actual implementation and outcomes of the listed initiatives. It is difficult to assess the number of initiatives listed in the Inventory, but as of September 2017, there seemed to be slightly less than 20 available online.

Global Cybersecurity Index (International Telecommunications Union)[8]

The first version of the Global Cybersecurity Index was released in 2014, with a second updated version published in 2017. This database rates the cybersecurity capacities of 194 countries across the five dimensions of legal measures, technical measures, organizational measures, capacity building, and cooperation that are further broken down by 25 indicators. The ITU makes it very clear that the GCI measures the commitment of countries through the actions they are taking rather than the impact their engagement is producing on users; such as providing increased levels of protection. 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 ranging from 0 to 1, with Singapore being the highest ranked country with a score of 0.925 (ITU 2017a). More detailed country profiles are available for download on the ITU's website[9], and an interactive tool also allows comparisons between a maximum of seven countries or regions[10]. However, the data tables are not offered for download.

INCYDER database (NATO Cooperative Cyber Defense Centre of Excellence)[11]

The International Cyber Developments Review (INCYDER) database lists legal and policy documents adopted by seventeen international and regional organizations such as the UN, the OECD, the G7, the EU, etc. The original documents are downloadable from the INCYDER platform and searchable

7 https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce
8 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
9 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
10 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_GLO_Graphics.aspx
11 https://ccdcoe.org/incyder.html

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 the scientific publications that discuss/evaluate these policies.

National Cyber Security Index (e-Governance Academy)[12]

The NCSI was launched in 2016 by the Estonian e-Governance Academy, with support from the Estonian government and international private sector partners. This two-year, EUR 200,000 project developed a methodology that seeks to measure countries' preparedness to prevent cyber threats, as well as their readiness to respond to cyber-attacks. The Index ranks 28 countries and is structured around 78 indicators arranged in the four groups of general cybersecurity, baseline cybersecurity, incident and crisis management, and international influence that are then further organised by twelve different capacities. Points are assigned depending on the level of capacity achieved[13]. Like in many other indexes, what gets measured is the existence of particular institutions and programs, not their effectiveness—or the lack thereof—to protect against cyber threats.

Other monitoring platforms are discussed in the ITU Index of Cybersecurity Indices (2017b). However, this focus mainly on threat metrics, user attitudes and business practices, and are less relevant to policy monitoring.

1.6. The limitations of existing policy monitoring tools

Although they are 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.

The proliferation of reports encourages a broader conversation among stakeholders and inspires further emulation to produce more relevant indicators and typologies; increasing the rate of knowledge transfer. However, there is also a risk that an overlap of efforts will result in unhealthy competition and confusing results. A quick comparison of the top ten countries appearing in the rankings published by the ITU and e-Governance Academy illustrates this point quite eloquently. Even though they use very similar indicators, they deliver diverging results and only agree on three countries as their top ten performers. The Czech Republic, which comes first in the NCSI ranking, barely comes in 35th position in the GCI.

[12] http://ncsi.ega.ee/
[13] http://ncsi.ega.ee/ncsi-index/#

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

Rank	GCI 2017	NCSI 2017
1.	Singapore	Czech Republic
2.	United States	Lithuania
3.	Malaysia	Georgia
4.	Oman	Belarus
5.	Estonia	Ukraine
6.	Mauritius	Moldova
7.	Australia	Latvia
8.	Georgia	Australia
9.	France	Canada
10.	Canada	Norway

The platforms reviewed above use countries as their unit of reference to produce aggregate scores or assessments. This approach supports global policy transfers but prevents researchers and decision makers from examining the discrete 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. In other words, 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 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 a direct relationship can be established between increased capacities and enhanced cybersecurity (Dutton et al. 2017), but a more granular understanding of what policies deliver which benefits, and how, remains elusive.

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

1.7. The Case for a Cybersecurity Policy Observatory

In light of the extensive policy surveillance knowledge developed in domains such as public health, education, violence and crime prevention, or environment protection, and considering how central cybersecurity has become to contemporary societies and the wellbeing of individuals and organizations, there seems to be an urgent need for the creation of a Cybersecurity Policy Observatory (CPO) that would complement the readiness and capacity monitoring initiatives discussed in the two previous sections.

The aim of the CPO would be to systematically collect detailed information about discrete cybersecurity policies in a format that would facilitate their cataloguing, retrieval, analysis and evaluation. This data would be updated regularly and be made available to independent researchers and policy makers to generate new insights on the effectiveness of existing policies, as well as their failures or counterproductive effects.

To assess the feasibility of this approach, a pilot study of 24 cybersecurity policies was conducted during the first half of 2017. This pilot was conducted at the Université de Montréal's International Centre of Comparative Criminology, with financial support from the Korean Institute of Criminology. The aims of this pilot were threefold:

1. Conduct a literature review of existing policy surveillance theories and practices, as well as a desktop analysis of a small sample of public health, education, criminal justice and cybersecurity policy monitoring platforms;

2. Leverage these findings to design a data capture framework that would incorporate the most relevant information and be refined throughout the pilot;

3. Apply this framework to a diversified sample of 24 cybersecurity policies and determine with a small team of research assistants the scalability of that approach.

To test the reliability and versatility of the data collection framework, the 24 cybersecurity policies selected to be included in the sample were sourced from eleven countries[14] and cover eleven common cybersecurity areas: legislation and regulation, privacy protection, law enforcement and crime prevention, standardization and accreditation, capacity building, education and workforce development, innovation and R&D, information sharing, public-private partnerships, economic incentives and nudging approaches, and public awareness. Diversity was the main selection criteria when selecting these countries.

[14] Australia, Canada, Estonia, France, Germany, Israel, Japan, Korea, the Netherlands, the UK, and the US.

We acknowledge that the limited resources and time available to conduct this pilot limited the size of our policy sample and introduced a geographical bias, attributable to the decision to work on policy summaries for which data was readily available. Yet, we believe it represents a useful tool to test the validity and robustness of our methodology, and to identify areas of improvement before future stages of the project.

1.8. Research workflow and coding methodology

Once the sample of policies was created, each policy was allocated to one of two research assistants who conducted extensive literature reviews through general online searches and access to more specialized academic databases. Once enough information had been collected or when searches did not produce new data, the information was processed and analyzed to produce policy summaries or profiles that are organized in four categories and 29 different entry fields. Table 2 gives an overview of the coding framework, while Annex 1 provides a more detailed description of the data found in each field.

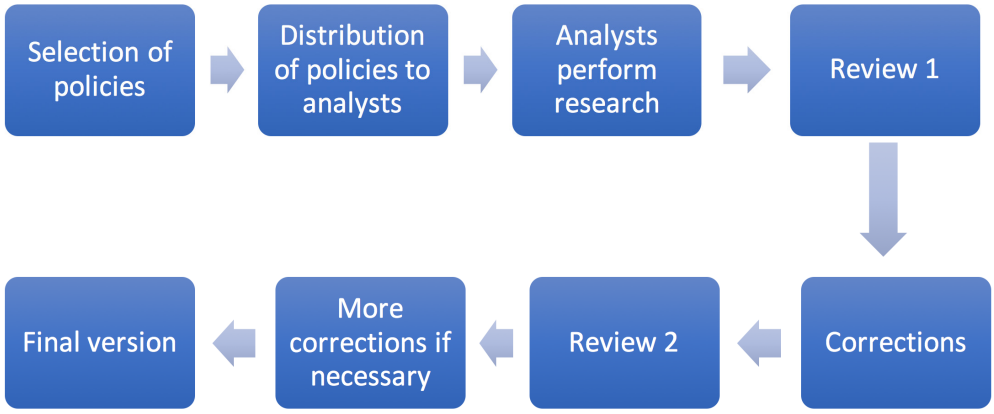
Table 3. Structure of the CPO Coding Framework

Categories	Data Fields
1. Overview of the policy and search filters	Summary Nature of the policy Related policies and legislation Keywords Snapshot data
2. 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
3. Evaluation of the policy	Existence of an evaluation Evaluation type Evaluator Methodology Outcomes

Categories	Data Fields
Additional information	URL Publications Media articles Documents

Once profiles were completed, they were reviewed by the project coordinator to identify inconsistencies across coders and to suggest improvements. Once the lead coder had implemented these changes, the principal investigator performed a final review and additional corrections or clarifications were made by the coding team. To ensure an additional layer of consistency and to enhance the level of feedback between coders, coordinator and principal investigator, a team meeting was scheduled every fortnight to raise coding issues and solve methodological dilemmas. Figure 1 provides an overview of the coding workflow.

Figure 1. Coding Workflow



The result of this pilot study are presented in the following section as 24 policy profiles that provide a glimpse of the most often cited cybersecurity policies, their features, and where available provide the evidence confirming their effectiveness, failure or suggesting the need to measure their outcomes more rigorously to better assess their impact on the digital ecosystem.

The final section discusses the lessons learned and the next possible steps in the creation of a Cybersecurity Policy Observatory.

2 Summaries of Cybersecurity Policies

List of the Countries

1. Australia
2. Canada
3. Estonia
4. France
5. Germany
6. Israel
7. Japan
8. Korea
9. Netherlands
10. UK
11. USA

Australia

1) Australian Internet Security Initiative (AISI)
2) Australia – Australian Cyber Security Growth Network (ACSGN)

Australia – Australian Internet Security Initiative (AISI)

1. Summary

The Australian Internet Security Initiative (AISI) is a program led by the Australian Communications and Media Authority (ACMA). Since 2005, the program has been gathering data from various sources on Australian internet protocol (IP) addresses that exhibit compromised behaviour. The AISI then provides Australian Internet Service Providers (ISPs) with a daily report on IP addresses in their networks that are assigned to potentially compromised machines. These reports help ISPs understand infections on their networks in order to better help customers clean their machines.

2. Nature

Anti-Botnet Strategy

3. Policy's Description

- **Date** : November 2005(Start of the Australian Internet Security Initiative)
- **Country** : Australia
- **Geographical scope** : Australia
- **Instigator** : Australian Communications and Media Authority (ACMA) Australian Government
- **Targeted issue / situation** :
  Malware infected computers and botnets can undertake harmful and criminal activities. There is a need for information on malware data, in particular on Australian infected IP addresses for ISPs to inform, advise and protect their customers.
- **Targeted population** :
  Australian ISPs, including universities and other online communications providers, as well as their customers.
- **Goals of the policy** :
  - The primary goal of the program is to identify and report cases of malware infections across Australia.
  - A secondary goal is to help ISPs inform affected customers of malware outbreaks and provides assistance and support to those in need.
- **Components of the policy** :
  The AISI collects data on IP addresses that exhibit compromised behaviour. The program retrieves data from various reputable sources, including Microsoft, The Shadowserver

Foundation, the SpamHaus Project and Team Cymru. The data is inspected and then compiled into reports that are sent to concerned ISPs. Because participation in the AISI is voluntary, this information is not sent to *all* Australian ISPs, but only the organizations that have signed up to participate in the program. Each participating ISP receives a daily report with information on IP addresses on their network that may be compromised. This allows ISPs to inform customers associated with affected IP addresses that they might be at risk. The ISP can explain the infection to the customer, provide advice and help the customer resolve the situation. ISPs also receive weekly "repeated sightings" reports with information on re-occurring infections on their networks. ISPs can also retrieve and download additional data than what is included in the reports on the AISI online portal, which is available to all AISI participants.

- **Agents in charge** :

  The Australian Communications and Media Authority (ACMA) administers the AISI program.
  The ACMA is a government agency responsible for the regulation of the internet, radio, telecommunications and broadcasting in Australia.
  In regard to the AISI, the ACMA:
  - Gathers and compiles network information data from different Participating organizations;
  - Writes and sends daily and weekly reports to ISPs;
  - Maintains the online portal;
  - Conducts internal research on the advancement of the initiative as well as participants' satisfaction with the program.

- **Costs** : N/A

- **Sources of funding** : Australian Communications and Media Authority (ACMA)
  Australian Government

- **Penalties** : No

- **Incentives** :

  Can create competition between ISPs. ISPs who are known to deliver infection information to customers faster and offer better infection resolution support may become more attractive to consumers.

- **Challenges** : N/A

4. Implementation Information

- November 2005: AISI launched by Australian Communications and Media Authority (ACMA).
- September 2012: ACMA publishes first internal survey with industry participants. Participating organizations call for changes to the program so they may access data beyond the daily email alert and support the creation of an online portal.

- November 2014: Online portal launched, providing easier access to data for participating ISPs.
- March 2015: A report published by the Vice Chief of the Defence Force recommends expansion of the AISI by making it mandatory for all Internet Service Providers (ISPs). At the time of publication, the AISI had 139 members covering 90% of Australia's internet traffic. The Defense Minister also recommends that voluntary ISP actions, such as notifying customers of a compromised IP address, should be made mandatory and based on a tiered approach which should always result in situation resolution. This would improve competition between ISPs as they could compete for best security practices, on top of bandwidth and price.
- October 2015: ACMA published a second internal survey. Participating organizations suggest changes to the online portal, including access to more detailed information on reported malware infections. They also request more information on how the data is captured, how customers are affected and what data the AISI is unable to provide.

  June 2017: The AISI has 146 members, including 128 ISPs and 18 educational institutions. Participation remains voluntary.

5. Evaluation

- **Existence of an evaluation** : Yes
- **Evaluation type** : Surveys, Internal.
- **Evaluator** :

1) Australian Communications and Media Authority. (2012). *The Australian Internet Security Initiative - provider responses to security-compromised computers: Interviews with industry participants*. Australian Government. Retrieved from: http://www.acma.gov.au/~/media/Cyber%20Security%20and%20UCE/Research/pdf/The%20Australian%20Internet%20Security%20Initiativeprovider%20responses%20to%20securitycompromised%20computers.pdf

2) Australian Communications and Media Authority. (2015). The Australian Internet Security Initiative Interviews with industry participants October 2015 reportJun17LowRes pdf.pdf. Australian Government. Retrieved from: http://www.acma.gov.au/~/media/Cyber%20Security%20and%20UCE/Research/pdf/The%20Australian%20Internet%20Security%20Initiative%20Interviews%20with%20industry%20participants%20October%202015%20reportJun17LowRes%20pdf.pdf

- **Methodology** :

ACMA staff interviewed 24 AISI participants over the phone between December 2011 and February 2012 and then again between February and March 2015. Interviewees were representative of a range of AISI participants across various states and of various sizes.

- **Outcomes** :

In 2012, the vast majority of AISI participants reported using the information provided in AISI reports and those who did not were small companies aiming to have the resources to do so eventually. Report consultation was split roughly three ways: some participants always consulted both the daily and weekly reports, while others consulted only the daily reports or only the weekly reports. Reports in general were found to be useful and accurate by participants. Almost all organizations that used the AISI reports took action to advise and even sometimes assist their customers. Most would notify customers via e-mail or telephone, but some would suspend internet services until the customer would notice. Participants requested more information from AISI reports, especially on the types of machines infected as it is often difficult for smaller ISPs to link the IP addresses provided by the AISI to specific machines or customers.

In 2015, the research also addressed the use of the AISI online portal. Only one fifth of participants reported using the portal, others were either aware of its existence and not using it or not aware of it at all. Those who chose not to use the portal were content with the information they were already receiving by email. Like the 2012 surveys, ISPs had a wide range of approaches to dealing with compromised client machines. Again, participants asked for more detailed information from the AISI reports to help them save time.

6. URL

http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

https://portal.aisi.acma.gov.au/

7. Publications

Butler, B., & Lachow, I. (2012). Multilateral approaches for improving global security in cyberspace. *Georgetown Journal of International Affairs*, 5–14. Retrieved from http://journal.georgetown.edu/wp-content/uploads/2015/07/gj12702_Butler_Lachow-CYBER-2012.pdf

Ito, Y. (2011). Making the Internet clean, safe and reliable: Asia Pacific regional collaboration activities. In *2011 Second Worldwide Cybersecurity Summit*, 1–3. Available at IEEE Xplore: http://ieeexplore.ieee.org/document/5978796/

Tully, S. (2012). Protecting Australian Cyberspace: Are Our International Lawyers Ready. *Australian International Law Journal, 19*, 49–78. Available at AustLii: http://www.austlii.edu.au/au/journals/AUIntLawJl/2012/4.html

Vratonjic, N., Manshaei, M. H., Raya, M., & Hubaux, J.-P. (2010). ISPs and Ad Networks Against

Botnet Fraud. In T. Alpcan, L. Buttyán, & J. S. Baras (Eds.), *Decision and game theory for security*, 149–167. Available at Springer: https://link.springer.com/chapter/10.1007/978-3-642-17197-0_10

8. Media Articles

Australian Communications and Media Authority. Working with internet providers to fight malware. October 9th, 2012. Retrieved from http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/working-with-internet-providers-to-fight-malware-i-acma

Australian Communications and Media Authority. Australians underrate the risks of malware. October 1st, 2013. Retrieved from http://www.acma.gov.au/Citizen/Internet/esecurity/Staying-safe-online/australians-underrate-the-risks-of-malware-1

Australian Communications and Media Authority. AISI provider responses to security-compromised computers. November 29th, 2013. Retrieved from http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/the-aisi provider-responses-to-securitycompromised-computers-acma

Australian Communications and Media Authority. Successful lift-off for AISI portal. December 16th, 2014. Retrieved from http://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Cybersecurity/Successful-lift-off-for-AISI-portal

Barwick, H. AISI members call for program improvements. October 10th, 2012. Retrieved from https://www.computerworld.com.au/article/438687/aisi_members_call_program_improvements/

Barwick, H. Australian Internet Security Initiative portal launched to help ISPs. November 28th, 2014. Retrieved from https://www.computerworld.com.au/article/560587/australian-internet-security-initiative-portal-launched-help-isps/

Barwick, H. ISPs request changes to Australian Internet Security Initiative. October 6th, 2015. Retrieved from https://www.computerworld.com.au/article/586064/acma-considers-improvements-australian-internet-security-initiative/

Braue, D. ACMA database keeps finger on Australia's malware pulse. May 21st, 2013. Retrieved from https://www.cso.com.au/article/462419/acma_database_keeps_finger_australia_malware_pulse/

Chanthadavong, A. ACMA hones in on malware with internet security portal. November 27th, 2014. Retrieved from http://www.zdnet.com/article/acma-hones-in-on-malware-with-internet-security-portal/

9. Documents

http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/aisi-malware-statistics-1

10. Related Law / Policies / Etc.

iCode – a voluntary cybersecurity code of practice developed in 2010 by the Internet Association with the ACMA and the Australian Government, currently led by Communications Alliance

Japan Cyber Clean Centre

Korean Computer Emergency Response Coordination Centre

German Anti-Botnet Advisory Centre

German Anti-Botnet Advisory Centre

11. Keywords

Botnets, Malware, Internet Service Providers, Public-Private Partnership, Voluntary Program, Online Portal, Information Sharing, Australia

12. Snapshot

- Targeted population: Internet Service Providers
- Geographical scope: Australia
- Policy type: Anti-Botnet Strategy
- Status: Active

Australia – Australian Cyber Security Growth Network (ACSGN)

1. Summary

The Australian Cyber Security Growth Network (ACSGN) is a government-backed, industry-led, not-for-profit company. Launched in early 2017, it aims to improve the Australian cybersecurity industry by connecting existing businesses and helping new start-ups thrive. The ACSGN released the Security Sector Competitiveness Plan in April 2017, which includes research on the historic and current state of the Australian cybersecurity market, as well as actions required to improve the industry. The company is set to receive over A$30 million until 2020 to achieve its goal of strengthening the Australian economy through cybersecurity research and development.

2. Nature

R&D & Economic Development

3. Policy's Description

- **Date** :
  - December 2016: Announcement of establishment of the Australian Cyber Security Growth Network (ACSGN).
  - Early 2017: The ACSGN is operational.
- **Country** : Australia
- **Geographical scope** : Australia primarily; International.
- **Instigator** :
  Minister for Industry, Innovation and Science and the Minister Assisting the Prime Minister on Cyber Security.
- **Targeted issue / situation** :
  The worldwide cybersecurity industry is rapidly growing and becoming increasingly diverse, sophisticated and competitive. The ACSGN seeks to generate economic growth opportunities for the country by closing the R&D gap with world leaders such as the U.S. and Israel. It will also improve startups' access to venture capital in order to accelerate the commercialization of innovation.
- **Targeted population** :
  Australian cybersecurity companies, recent cybersecurity graduates, policy makers.
- **Goals of the policy** :
  The ACSGN would like to develop an internationally-respected, technically advanced Australian cybersecurity industry. More precisely, the Network aims to triple the size of Australian

cybersecurity industry sector, from A$2 billion to A$6 billion by contributing to three specific key goals:

1) Create an Australian cyber security ecosystem;
2) Export Australia's cybersecurity to the world and;
3) Make Australia the leading centre for cyber education.

- **Components of the policy** :

The Australian Cyber Security Growth Network published a report in April 2017 titled the Cyber Security Sector Competitiveness Plan. This plan provides research on the existing Australian cybersecurity industry and details how it aims to contribute to its three key goals. Each goal is divided into strategies, which are then broken down into actions. Each action has a lead actor: the ASCGN, Government or Industry. In order to fulfil each strategy and accomplish its three key goals, the ASCGN is designed to act as a *multiplier* and a *connector* for the Australian cyber security market.

It aims to help multiply the market by making it easier for start-ups to find capital and business-building information and to help connect the market by linking industry and government, not only within Australia, but internationally.

1) Grow an Australian cyber security ecosystem:
   - Help Australian cyber startups find their first customers by providing business coaching and undertaking showcases;
   - Create a network of researchers and organizational practitioners to connect research and industry;
   - Form a panel of C-Suite professionals and attract additional funding sources that can help back and finance new cyber startups;
   - Analyze existing cybersecurity contracts and provide recommendations.

2) Export Australia's cybersecurity to the world:
   - Work with government and education/training institutions to better understand Australian cyber security export opportunities and potential international target markets.

3) Make Australia the leading centre for cyber education:
   - Work with government to improve the information in high schools on cybersecurity career paths, especially for women;
   - Work with industry to create a post-secondary program in which young professionals can gain work experience in cybersecurity;
   - Along with industry, create cyber challenges, training courses and apprenticeship models for cyber security that will help hire more graduates.

Though not yet available, the ASCGN is set out to develop a set of metrics to ensure that it is able to measure how far along it is in reaching its goals.

- **Agents in charge** :
  The ACSGN was established and is funded by the Department of Industry, Innovation and Science under the Industry Growth Centres Initiative. However, the ACSGN itself is an independent, not-for-profit entity. It is composed of an industry-led board and collaborates with cybersecurity industry specialists, policymakers and researchers.
- **Costs** : A$31.9 million through 2019-20.
- **Sources of funding** : Department of Industry, Innovation & Science; Australian Government.
- **Penalties** : N/A
- **Incentives** : N/A
- **Challenges** : N/A

4. Implementation Information

- December 2015: Announcement of ACSGN as part of National Innovation and Science Agenda.
- December 2016: Announcement of establishment of ACSGN.
- Early 2017: ACSGN is operational.
- April 2017: Launch of Cyber Security Sector Competitiveness Plan, announced by the Minister for Industry, Innovation and Science.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.acsgn.com/

7. Publications

Caelli, W. J., & Liu, V. (2017). Cybersecurity education at formal university level: An Australian perspective. In *Science & Engineering Faculty*. Las Vegas, NV. Retrieved from https://eprints.qut.edu.au/106424/

8. Media Articles

Australian Government. New Growth Centre to help Australia become a global cyber security leader. December 5th, 2016. Retrieved from http://www.minister.industry.gov.au/ministers/hunt/media-releases/new-growth-centre-help-australia-become-global-cyber-security-leader

Braue, D. "There won't be a more passionate advocate" for Australian security innovation, new ACSGN head vows. December 6th, 2016. Retrieved from https://www.cso.com.au/article/611166/there-won-t-more-passionate-advocate-australian-security-innovation-new-acsgn-head-vows/

Corner, S. Meet the man charged with growing Australia's cyber security industry. April 21st, 2017. Retrieved from https://www.computerworld.com.au/article/618029/meet-man-charged-growing-australia-cyber-security-industry/

Pearce, R. Roadmap seeks to boost local cyber security industry. April 20th, 2017. Retrieved from https://www.computerworld.com.au/article/617909/roadmap-seeks-boost-local-cyber-security-industry/

Stilgherrian. Australia's bold plan for cybersecurity growth. April 20th, 2017. Retrieved from http://www.zdnet.com/article/australias-bold-plan-for-cybersecurity-growth/

9. Documents

Australian Cyber Security Growth Network. (2017). Cyber Security Sector Competitiveness Plan. Retrieved from https://www.acsgn.com/wp-content/uploads/2017/04/Cyber-Security-SCP-April2017.pdf

10. Related Law / Policies / Etc.

Australia's Cyber Security Strategy 2016

11. Keywords

Cybersecurity Industry, Economic Growth, Public-Private Partnership, Workforce Development, Innovation, R&D

12. Snapshot

- Targeted population: Cybersecurity industry
- Geographical scope: Australia
- Policy type: R&D & Economic Development
- Status: Active

Canada

1) Canadian Anti-Spam Legislation (CASL)
2) Cyber Incident Response Center (CCIRC)
3) Canadian Cyber Threat Exchange (CCTX)
4) Digital Privacy Act (DPA)

Canada – Canadian Anti-Spam Legislation (CASL)

1. Summary

Canada's anti-spam legislation (CASL) regulates how businesses can use electronic tools for communication promotion purposes, and is aimed at protecting consumers against spam and electronic threats such as botnets. The law makes it illegal for companies to send commercial electronic messages, to install programs such as malwares on someone's computer, or to collect data, without consent. Consumers affected by those practices can file a complaint with the Canadian Radio-Television and Telecommunications Commission (CRTC), the regulatory and enforcement agency in charge of issuing administrative and monetary penalties for violations of the law. Initially, the law was supposed to make it possible for consumers to bring a private right of action in court, but this section of the law has been suspended in July 2017.

2. Nature

Regulation and Legislation

3. Policy's Description

- **Date** :
  - May 2010: Bill passed.
  - July 2014: Bill entered into force.
- **Country** : Canada
- **Geographical scope** : Canada
- **Instigator** : Industry Canada (Now ISED)
- **Targeted issue / situation** :
  More and more consumers receive spam emails, which can lead to identity theft and fraud. The Canadian government is looking to protect Canadian citizens from these threats.
- **Targeted population** :
  Businesses and organizations that are sending promotional emails, collecting personal information or installing unsolicited computer programs.
- **Goals of the policy** :
  The main goal is to protect consumers against spam emails, electronic threats and the misuse of digital technology.
  The secondary goal is ensuring businesses remain competitive in a global digital marketplace.
- **Components of the policy** :
  The law makes it illegal for companies to:

- Send of commercial electronic messages without the recipient's consent (permission), including messages to email addresses and social networking accounts, and text messages sent to a cell phone;
- Engage in the alteration of transmission data in an electronic message which results in the message being delivered to a different destination without express consent;
- Install computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee (added in January 2015);
- Use false or misleading representations online in the promotion of products or services;
- Collect personal information through accessing a computer system in violation of federal law (e.g. the Criminal Code of Canada); and
- Collect electronic addresses by the use of computer programs or the use of such addresses, without permission (address harvesting).

Consumers affected by those practices can fill a complaint with the CRTC, which can then investigate to determine if the individual or organization has violated the law, and eventually seek damages.

The law also allows individuals and organizations affected by an act or omission in contravention of the law to bring a private right of action in court against individuals and organizations whom they allege have violated the law. However, this section of the law which was supposed to enter into force on July 1st 2017 has been suspended.

- **Agents in charge** :

Three government agencies are responsible for enforcing the law:

1) The Canadian Radio-Television and Telecommunications Commission (CRTC) has the primary enforcement responsibility. It receives consumer complaints, and is also in charge of investigating, taking appropriate action, and setting administrative monetary penalties for violations of the law (sending non-compliant commercial electronic messages ; altering transmission data without express consent ; installing a computer program on a computer system or network without content);
2) The Competition Bureau, an independent law enforcement agency, is able to address false and misleading representations and deceptive marketing practices in the electronic marketplace (including false or misleading sender or subject matter information, electronic messages and locator information);
3) The Office of the Privacy Commissioner protects the personal information of Canadians. It enforces the legislation with respect to the collection of personal information through access to computer systems and electronic address harvesting where bulk email lists are compiled through mechanisms.

- **Costs** : Unknown
- **Sources of funding** : Canadian Federal Government
- **Penalties** :
  - When the CRTC is made aware of a violation, it has several options. It can issue a Notice of Violation, or seek actual and statutory damages.
  - The CRTC may levy fines of up to CAD 1 million for an individual or CAD 10 million for a business that contravenes the Act.
  - Between 2014 and 2017 the CRTC has imposed fines for an amount of CAD 1,558,000 to Canadian companies for CASL violations (Compufinder, Porter Airlines, Rogers, Kellogg, Pentyoffish, M. William Rapanos).
- **Challenges** :

  The Canadian Federation of Independent Business (CFIB), a group of private companies opposed to the law because companies sending spams could be sued. Companies are afraid of being sued, as there is a risk that they would have to pay legal fees. This would damage their reputation, and had negative economic consequences (lower sales, damaged brand image…). They ask the suspension of the private right of action.

4. Implementation Information

- January 2014: Bill entered into force.
- January 2015: additional section of the act coming into force. It is now forbidden to install computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee.
- July 2017: Sections that deal with the private right of action have been suspended.
- Between 2014 and 2017 the CRTC has imposed fines for an amount of CAD 1,558,000 to Canadian companies for CASL violations (Compufinder, Porter Airlines, Rogers, Kellogg, Pentyoffish, M. William Rapanos).

  Several notices of violations were noted by the CRTC but not disclosed to the public.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html

7. Publications

Crowne, E., & Provato, S. (2014). Canada's Anti-Spam Legislation: A Constitutional Analysis. John Marshall Journal of Information Technology & Privacy Law, 31(1). Available at SSRN: https://ssrn.com/abstract=2523985

Neogi, P., & Cordell, A. (2010). The Internet and the Need for Governance: Learning from the Past, Coping with the Future. Journal of Internet Banking and Commerce, 15(2). https://pdfs.semanticscholar.org/8f9d/632b7fcc15255265ace6d4198c557e38c3cb.pdf

8. Media Articles

Mochrie, D. Overview of Canada's Anti-Spam/Anti-Spyware Legislation and How It Impacts Franchisors. May 2014. Osler Company website. https://www.osler.com/en/resources/regulations/2014/franchise-review-may-2014/overview-of-canada-s-anti-spam-anti-spyware-legisl

Bouw, B. New anti-spam law 'a big deal' for small business. March, 24th, 2014. The Globe and Mail Canada.

http://www.theglobeandmail.com/report-on-business/small-business/sb-managing/businesses-rush-to-comply-with-tough-new-anti-spam-law/article17609044/

Krashinsky Robertson, S. Canadian companies still sending unwanted emails after anti-spam law. July, 9th, 2014. The Globe and Mail Canada. http://www.theglobeandmail.com/report-on-business/industry-news/marketing/canadian-companies-still-sending-unwanted-e-mails-after-anti-spam-law/article19535536/

Miller, J. Canada's anti-spam rule slashes companies' email lists. July, 24th, 2014. The Financial Post. http://business.financialpost.com/entrepreneur/canadas-anti-spam-slashes-companys-email-lists

Melnitzer, J. Understanding CASL's computer download rules is the key to avoiding them. November 27th, 2014. The Financial Post. http://business.financialpost.com/legal-post/understanding-casls-computer-download-rules-is-the-key-to-avoiding-them

9. Documents

N/A

10. Related Law / Policies / Etc.

N/A

11. Keywords

Canada, Spam, Malware, Personal Information, Consent, Telecommunications, Commercial Electronic Message, Email Newsletters

12. Snapshot

- Targeted population: businesses and organizations
- Geographical scope: Canada
- Policy type: Regulation and Legislation
- Status: Active

Canada – Cyber Incident Response Center (CCIRC)

1. Summary

The Canadian Cyber Incident Response Centre (CCIRC) is Canada's cyber security incident response team. It acts as a coordination center that is responsible for ensuring the security and resilience of cyber systems outside the federal government. It provides advice, support, and coordinates information sharing and incident response. CCIRC works with a group of public and private partners, as well as with counterpart foreign cybersecurity incident response units.

2. Nature

Information Sharing; Capacity Building.

3. Policy's Description

- **Date** :
  - 2003: Creation of CCIRC (within Public Safety Canada).
- **Country** : Canada
- **Geographical scope** : Canada
- **Instigator** : Public Safety Canada
- **Targeted issue / situation** :
  The increasing number of cyber threats and cyber-attacks that are faced by Canadian provincial and municipal governments, as well as private critical infrastructure operators such as utilities, banks or telecommunications service providers.
- **Targeted population** :
  National non-federal governments (provincial and municipal) and critical infrastructure sectors (banks, phone service providers, companies involved in the delivery of electricity, petroleum production, water, and transportation).
- **Goals of the policy** :
  - The primary goal of the program is to monitor cyber threats.
  - The second goal of the program is to coordinate the national response to any cyber security incident.
- **Components of the policy** :
  CCIRC is a national coordination center responsible for reducing the exposure of Canadian stakeholders to cyber risks. Governments or companies can contact CCIRC, which will provide:
  - Advice and support for prevention: publication of cyber security bulletins, technical reports

and security guidelines;

- Technical advice and support in case of an attack: publication of alerts and technical reports on an ongoing basis to help its partners take appropriate protective measures;
- Information sharing: CCIRC uses the "Traffic Light Protocol" for cyber awareness products shared with their partners (Red: no sharing; Amber: limited sharing; Green: private sharing; White: no restrictions).

- **Agents in charge** :
  1) CCIRC operates from within Public Safety Canada.
  2) CCIRC relies on a broad group of partners from diverse horizons: the federal government, provinces, territories, municipalities, critical infrastructure organizations, academia and foreign governments and organizations.
- **Costs** : Not found
- **Sources of funding** : Public Safety Canada, Canadian government.
- **Penalties** : No
- **Incentives** : No
- **Challenges** : No

4. Implementation Information

- 2005: creation CCIRC, within Public Safety Canada.
- 2011: the government clarified the role of the CCIRC.
- 2012 and 2016: the capacity of CCIRC was increased as a result of higher federal funding.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

7. Publications

Government of Canada, (2013). *Cyber Incident Management Framework for Canada. Government of Canada.*
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/cbr-ncdnt-frmwrk-eng.pdf

8. Media Articles

Solomon, H. Canada's national cyber threat centre looking to expand. March 16th, 2016. It world Canada.
http://www.itworldcanada.com/article/canadas-national-cyber-threat-centre-looking-to-expand/381641

Joseph, R. Canada's Cybersecurity needs work, despite high ranking: expert. July 6th, 2017. Globalnews.
http://globalnews.ca/news/3580397/canadas-cybersecurity-needs-work-despite-high-ranking-expert/

9. Documents

N/A

10. Related Law / Policies / Etc.

Canada's Cyber Security Strategy 2010
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

11. Keywords

Cyber Threats, Cyber Incidents, Incident Response, Information Sharing, Coordination

12. Snapshot

- Targeted population: Canada's non-federal key systems and critical infrastructure sectors (banks, telecommunications, energy providers…)
- Geographical scope: Canada
- Policy type: Information sharing, Incident response, Capacity building
- Status: Active

Canada – Canadian Cyber Threat Exchange (CCTX)

1. Summary

The Canadian Cyber Threat Exchange (CCTX) is an independent, non-profit organization that aims to increase information sharing between private Canadian companies, government departments and institutions. Launched in December 2016, the CCTX offers an array of services to its subscribers based on their size. Subscribers pay an annual subscription fee to become either Members or Associates. All subscribers gain access to the cyber intelligence generated by the CCTX; however, Members have unique privileges that grant them greater access to the CCTX databases and governing power over CCTX decision-making.

2. Nature

Information Sharing

3. Policy's Description

- **Date** :
  - December 2016: Official launch of Canadian Cyber Threat Exchange (CCTX).
- **Country** : Canada
- **Geographical scope** : Canada
- **Instigator** :
  The CCTX was instigated by the Canadian Council of Chief Executives. Air Canada, Bell Canada, Canadian National Railway Company, HydroOne, Manulife, Royal Bank of Canada, Telus, TD Bank Group and TransCanada Corporation are the founding members of the CCTX.
- **Targeted issue / situation** :
  Cybercrimes, such as online fraud, identity theft and ransom are on the rise worldwide, but may be underreported in Canada. There are already several sector-specific information sharing centres in Canada; however, there is a need for a cross-sector information centre that would encourage Canadian companies to increase cybersecurity information sharing.
- **Targeted population** :
  Private Canadian businesses and multi-national organizations conducting business in Canada; governmental departments; different private or public institutions (health, academic, law enforcement, etc.).
- **Goals of the policy** :
  The Canadian Cyber Threat Exchange aims to increase cross-sector information sharing between Canadian businesses and, eventually, the Canadian government.

- **Components of the policy** :

The CCTX operates the CCTX "Data Exchange" which provides different forms of anonymized threat and vulnerability data. This data comes from companies that are subscribed to the CCTX, as well as from government and commercial sources. The CCTX sorts, analyzes, processes, and distributes this threat data to its subscribers as actionable intelligence. It shares this contextualized information along with mitigation options and operational tools through e-mail reports and a document repository.

The CCTX also operates a "Collaboration Centre", which is an exclusive forum for subscribers where best practices, techniques, insights and expertise can be exchanged and discussed. Together, these services seem to comprise what the CCTX calls on its website "the Knowledgebase".

All subscribers:

- gain access to CCTX knowledge;
- receive passes to the CCTX Annual conference and participate in committees and workgroups;
- receive alerts, bulletins, advisories, newsletters and other communications.

The Canadian Cyber Threat Exchange (CCTX) recognizes two types of subscriber statuses: members and associates. Members have unlimited access to the knowledge databases whereas associates receive a defined number of consultations. Members also obtain more passes to the annual conference than associates. In addition to these privileges, members may also nominate a representative to the CCTX Board and participate in Circles of Trust and can contribute to the CCTX's communications.

Within member and associate subscriber statuses are different sub-levels of services available. Members and associates of different sizes and affiliations (e.g.: large, medium or small businesses; academic, medical or municipal associations) and business associations can participate as CCTX affiliates, with partial benefits.

- **Agents in charge** :

1) Day-to-day operations of the Canadian Cyber Threat Exchange (CCTX) are led by Executive Director Robert (Bob) Gordon. Gordon has occupied numerous senior leadership positions in both the public and private sector, including acting as Public Safety Canada's Special Advisor on Cyber Security and as Director of Global Cyber Security at CGI.
2) EWA Canadian is the Managed Security Service Provider of the CCTX and is responsible for infrastructure and analytics.
3) The CCTX is governed by its members through the Board of Directors. Members elect directors who then serve two-year terms. Any member can apply to run as director. The Board Chair is currently Marc Duchesne of Bell Canada.

- **Costs** :
  The annual CCTX Member fee is CAD 50,000. Medium-sized businesses and institutions may join as associates for CAD 20,000 per year and small businesses may also join as associates but for as little as CAD 2000 a year.
- **Sources of funding** : The CCTX is funded by the annual fees paid by members and associates.
- **Penalties** : N/A
- **Incentives** : N/A
- **Challenges** : N/A

4. Implementation Information

- December 2015: The Canadian Council of Chief Executives along with the founding members announces the development of the Canadian Cyber Threat Exchange (CCTX).
- January 2016: CCTX begins recruiting additional members.
- April 2016: CCTX announces Request for Proposal, seeking to identify interested suppliers providing a cyber threat information service. Robert (Bob) Gordon is announced as the first Executive Director.
- December 2016: CCTX issues first national threat report at its inaugural annual symposium; introduces lower fees for small businesses; announces online portal and setup of collaborative space for members.
- February 2017: CCTX is fully operational with all available services.
- August 2017: The CCTX is in the process of partnering with Public Safety Canada and the Canadian Communications Security Establishment to initiate automated information sharing.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://cctx.ca/

7. Review

N/A

8. Media Articles

Barth, B. Canadian Cyber Threat Exchange to select its MSP by end of month. June 4th, 2016. Retrieved from: https://www.scmagazine.com/news/canadian-cyber-threat-exchange-to-select-its-msp-by-end-of-month/article/528242/

Business Council of Canada. Business community unites to fight cyber threats. December 11th, 2015. Retrieved from: http://thebusinesscouncil.ca/news/business-community-unites-fight-cyber-threats/

Canada Newswire. The Canadian Cyber Threat Exchange (CCTX) is operational and reaching out to Canadian businesses. December 9th, 2016. Retrieved from: http://www.newswire.ca/news-releases/the-canadian-cyber-threat-exchange-cctx-is-operational-and-reaching-out-to-canadian-businesses-605666706.html

Continuity Central. Canadian Cyber Threat Exchange to be launched in 2016. December 15th, 2015. Retrieved from: http://www.continuitycentral.com/index.php/news/technology/747-canadian-cyber-threat-exchange

Reid, S. Canadian companies have a big new ally in the fight against cyber crime. December 11th, 2015. Retrieved from: http://business.financialpost.com/technology/canadian-companies-have-a-big-new-ally-in-the-fight-against-cyber-crime

Seglins, D. New cybersecurity network aims to share data on emerging threats. December 11th, 2015. Retrieved from: http://www.cbc.ca/news/technology/cyber-security-cctx-network-1.3360119

Solomon, H. Canadian threat exchange vows to give unique value to members. June 1st, 2016. Retrieved from: http://www.itworldcanada.com/article/canadian-threat-exchange-vows-to-give-unique-value-to-members/383799

Solomon, H. Canadian Cyber Threat Exchange ready to start membership push. December 8th, 2016. Retrieved from: http://www.itworldcanada.com/article/canadian-cyber-threat-exchange-ready-to-start-membership-push/389034

Solomon, H. Ottawa about to join cyber threat exchange. August 8th, 2017. Retrieved from: http://www.itworldcanada.com/article/ottawa-about-to-join-cyber-threat-exchange/395459

9. Documents

N/A

10. Related Law / Policies / Etc.

N/A

11. Keywords

Information Sharing, Threat Intelligence, Incident Response

12. Snapshot

- Targeted population: Private companies; government departments
- Geographical scope: Canada
- Policy type: Information sharing
- Status: Active

Canada – Digital Privacy Act (DPA)

1. Summary

Canada's Digital Privacy Act, passed in 2015, is an amendment to the Personal Information Protection and Electronic Documents Act (hereafter PIPEDA), which was passed in 2000. This bill aims at protecting the privacy of consumers by limiting the collections, use and communication of personal information as part of commercial activities by public or private organizations.

The DPA reinforces this consumer protection by increasing the powers of the Privacy Commissioner in charge of the implementation of the law, by adding legal obligations for organizations, and by making it unlawful to be found in non-compliance with data security regulations.

2. Nature

Regulation and Legislation; Privacy Protection.

3. Policy's Description

- **Date** :
  - June 2015: DPA (Bill S-4) passed.
- **Country** : Canada
- **Geographical scope** : Canada
- **Instigator** : Canadian government
- **Targeted issue / situation** :
  The circulation and exchange of personal information is facilitated by technology; it can be collected by companies and shared with third-parties without appropriate consent.
- **Targeted population** :
  Public or private organizations as part of their commercial activities.
- **Goals of the policy** :
  - PIPEDA goal: to protect the right to privacy of vulnerable customers.
  - DPA goal: to enhance these protections.
- **Components of the policy** :
  - Organizations have to contact people affected by a security breach and have to report the "breach of security safeguards" to the Privacy Commissioner. If organizations don't comply with their obligations, they're committing a crime and risk a fine of up to CAD 100,000.
  - DPA changes the notion of consent of the consumers. The consent is now valid "only if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting" (section 6.1).

- Organizations are exempted to require consumers' consent for sharing information in case of a federal investigation, commercial transaction, insurance claim, or if the information is produced in the course of employment or business.

- **Agents in charge** :

1) The Office of the Privacy Commissioner of Canada was created in 1983 by the Privacy Act. It is a government agency, which is responsible for the implementation of PIPEDA. It is in charge of receiving and processing complaints from the public or organizations.
2) The Privacy Commissioner can enter into compliance agreements with organizations, and is also able to initiate court proceedings (added since DPA was passed) if the organization fails to meet its obligations under the agreement.

- **Costs** : Not found
- **Sources of funding** : Government of Canada
- **Penalties** :

DPA introduced fines up to CAD 100,000 if organizations don't disclose a data breach that reaches a certain threshold.

- **Incentives** : N/A
- **Challenges** :

Some law professors and lawyers pointed out that certain new provisions such as exceptions to requirements of consent could threaten consumers' right to privacy.

4. Implementation Information

- 1983: Creation of the Office of the Privacy Commissioner (with the Privacy Act).
- 2000: PIPEDA enacted.
- 2010 and 2012: attempt to reform PIPEDA (died in the order paper).
- 2015: DPA enacted.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

http://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html

7. Publications

N/A

8. Media Articles

Glover, D., Morgan, C., Sookman, B, & Thompson, K. Digital Privacy Act is now law. June 19, 2015. McCarthy Tetrault blog. Retrieved from http://www.mccarthy.ca/article_detail.aspx?id=7117

Fougere, M. Canada's Digital Privacy Act: New carrots and sticks to promote compliance with Canadian privacy legislation or a safe heaven for expanded information sharing ? July 2014. Norton Rose Fulbright blog. Retrieved from http://www.nortonrosefulbright.com/knowledge/publications/119103/canadas-digital-privacy-act-new-carrots-and-sticks-to-promote-compliance-with-canadian-privacy-legislation-o

Graton, E. New Requirements of the Digital Privacy Act (Bill S-4). June 19, 2015. Borden Ladner Gervais blog. Retrieved from http://blg.com/en/News-And-Publications/Publication_4153

Tencer, D. Bill S-4, Tories' Digital Privacy Act, An Attack on Digital Privacy: Critics. April 14, 2014. Huffington post Canada. Retrieved from http://www.huffingtonpost.ca/2014/04/14/digital-privacy-act-canada_n_5147704.html?utm_hp_ref=ca-digital-privacy-act

9. Documents

https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=6524311

10. Related Law / Policies / Etc.

PIPEDA (Personal Information Protection and Electronic Documents Act)
http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-4

Office of the Privacy Commissioner of Canada
https://www.priv.gc.ca/en

11. Keywords

Privacy, Consent, Personal Information, Data Breach Disclosure

12. Snapshot

- Targeted population: Public and private organizations
- Geographical scope: Canada
- Policy type: Privacy protection
- Status: Active

Estonia

Cyber Defence League

Estonia – Cyber Defence League

1. Summary

The Cyber Defence League is a unit of the Estonian Defence League that involves the participation of civilians to cyber operations on a voluntary basis in case of a national emergency. The volunteers are mostly IT experts, but can also include educators, lawyers, and economists. The volunteers are trained to be ready in case of a cyber emergency and can be mobilized within 24h, and answer to military operations.

2. Nature

Capacity Building; Education and Workforce Development; Public Awareness.

3. Policy's Description

- **Date** :
  - 2011: A Cyber Defence Unit was formally added to the existing Estonian Defence League.
  - May 2013: Enforcement of the new Defence League Act.
- **Country** : Estonia
- **Geographical scope** : Estonia
- **Instigator** : Ministry of Defence, Estonian government
- **Targeted issue / situation** :

  Estonia is one of the most wired country reliant on cyber services, making it extremely vulnerable to cyber-attacks. In 2007, the country suffered what was then one of the biggest cyber-attacks in history. Banks', parliament's and government websites were flooded with data. It was concluded that the attack originated from Russia, though this act of cyberwar could not be linked to the Russia government.
- **Targeted population** :

  Estonia's cyber infrastructures, such as government, banking, utilities, news and broadcasting networks.
- **Goals of the policy** :

  The CDU mission is to protect "Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of national defence" (Kaska et al., 2013). There are 3 main secondary objectives:

  1. Developing a network of cooperation, also for crisis response:
     - Development of cooperation among qualified volunteer IT specialists;
     - Creation of a network which facilitates public private partnership and enhances preparedness

in operating during a crisis situation.

2. Improving the security of critical infrastructure through the dissemination of knowledge and training.
3. Promoting awareness, education and training:
   - Education and training in information security;
   - Participation in international cyber security training events.

- **Components of the policy** :

1) Membership procedure:
   - Firstly, to be part of the Cyber Unit, there are requirements to become a member. The criteria for membership are: be at least 18 years-old, be an Estonian citizen, have an impeccable record, have a good health, be loyal to the Estonian Republic and recognize the independence and constitutional order of Estonia, have knowledge and experience in information security (not only technical knowledge, but also in the legal, policy or education spheres). The members applying to be part of the Cyber Defence Unit must also give two references from morally responsible referees;
   - The applicants must submit a written request, accompanied by a recommendation from a member of the Defence League. The application process includes a background check, and upon acceptance, an oath of loyalty must be taken;
   - Since membership is on a voluntary basis, members are not obligated to participate in a particular activity of the Defence League. Their voluntary contribution implies freedom to decide on their participation, and their involvement is rather enforced by moral than regulatory means.

2) Activities and duties might include:
   - Support police activities in countering cyber threats;
   - Assist and support in rescue events or operations, engage in resolving emergencies;
   - Engaged in case of a state of national emergency.

   For each of these activities, the members must undergo a period of relevant training.

3) Tasks and activities relevant for the cyber unit:
   - Core tasks: education and training
     - Improving the skills, knowledge, attitude and experience of members;
     - Organisation of seminars, training events, information sharing, field studies;
     - Participation in military training;
     - Cyber defence exercises and overall defence and crisis management exercises;
     - Regular weekend exercises.
   - Core tasks: strengthening and ensuring the security of the population
     - Supply malware screening solutions for public school computers;

- ○ Assist with the installation and security testing of the electronic voting system in Estonia;
- ○ Offering professional expertise for preventive purpose.

- Supplementary tasks: cyber security assistance
  - ○ A draft regulation of the CDU includes a wide range of measures both passive (data monitoring and malware analysis) and active (security testing ICT solutions, threat mitigation, cybercrime prevention, reverse engineering, network traffic analysis);
- Supplementary tasks: cyber security in emergency and crisis
  - ○ The CDU may be used in prevention of damage to objects of high-risks of attacks, such as: building and equipment for vital services, physical damage or destruction that would impair continuous operation of the entire vital service;
  - ○ Prevention or countering certain criminal offences such as acts related to terrorism.

- **Agents in charge** :

1) The Cyber Defence Unit is part of the Estonian Defence League, which is in turn, part of the National Defence Organisation. The Defence League is a voluntary national defence organisation that operates within the Ministry of Defence. The Defence League is also an independent legal entity that engages in economic, educational and organisational activities. Since the Cyber Unit is a structural part of the Defence League, it has no independent legal capacity.

2) The Commander of the Cyber Defence Unit answers to the Commander of the Defence League. The cyber unit has its own personnel, a team led by a Chief of Staff who reports to the Commander of the cyber unit. The unit is mostly comprised of volunteers (over a hundred) and also paid employees (3). They include specialists in essential cyber security positions in national infrastructure, experts in IT, skilled in technology patriotic individuals, and specialists in other fields related to cyber security, such as economy, law, etc. (Kaska et al., 2013; Estonian Defence League's Cyber Unit, 2017).

3) The exact number of volunteers is classified, but it might represent 1% of all specialists in cybersecurity in Estonia.

- **Costs** : Unknown
- **Sources of funding** : Mainly government funds
- **Penalties** : N/A
- **Incentives** : N/A
- **Challenges** : No

4. Implementation Information

- September 2007: the idea to form a Cyber Defence League is suggested.
- Shortly after: creation of an informal cooperation network within the Estonian Defence League.
- 2009: two cyber defense sub-units are created, in Tartu and Tallinn.
- 2010: field studies since then.
- 2011: the sub-units are assembled and the Cyber Defence Unit is created and formally added to the existing Estonian Defence League.
- May 2013: Enforcement of the new Defence League Act.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

http://www.kaitseliit.ee/en/cyber-unit

https://www.riigiteataja.ee/en/eli/525112013006/consolide

https://www.eesti.ee/en/security-and-defense/voluntary-participation-in-national-defence/estonian-defence-league/

7. Publications

Kaska, K., Osula, A.-M., & LTC Stinissen, J. (2013). The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis, NATO Cooperative Cyber Defence Centre of Excellence, 1-45. Available at: https://ccdcoe.org/multimedia/cyber-defence-unit-estonian-defence-league-legal-policy-and-organisational-analysis-0.html

Cardash, S., Cilluffo, F. J., & Ottis, R. (2013). Estonia's Cyber Defence League: A Model for the United States? *Studies in Conflict & Terrorism, 36*(9), 777-787. DOI: 10.1080/1057610X.2013.813273. Available at: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2013.813273

Shackelford, S. J., & Andres, R. B. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Georgetown Journal of International Law, 42*, 971-1016.

Available at:
http://heinonline.org/HOL/Page?handle=hein.journals/geojintl42&div=35&g_sent=1&collection=journals

Jackson, C. M. (2013). Estonian cyber policy after the 2007 attacks: Drivers of change and factors for success. *New Voices in Public Policy, 7*(1), 1-15. Available at:
http://journals.gmu.edu/newvoices/article/view/69

Lipke, A. (2016). *US and NATO Cyber Defense: Bridging the Resource Gap with a Centralized Market Structure* (Doctoral dissertation, The George Washington University). Available at:
https://search.proquest.com/docview/1870036568?pq-origsite=gscholar

8. Media Articles

Fedorov, A. Estonia recruits hundreds for its Defence League Cyber Unit. May 1st, 2015. Retrieved from:
https://www.scmagazineuk.com/estonia-recruits-hundreds-for-its-defence-league-cyber-unit/article/537336/

Blair, D. Estonia recruits volunteer army of 'cyber warriors'. April 26th, 2015. Retrieved from: http://www.telegraph.co.uk/news/worldnews/europe/estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html

Gjelten, T. Volunteer Cyber Army Emerges In Estonia. January 4th, 2011. Retrieved from:
http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation

Maldre, P. Estonia's role in NATO's growing cyber capability. September 14th, 2016. Retrieved from: http://estonianworld.com/security/estonias-role-natos-growing-cyber-capability-2/

Kenyon, H. Volunteer cyber corps to defend Estonia in wartime. January 12th, 2011. Retrieved from: https://defensesystems.com/articles/2011/01/12/estonia-cyber-defense-league-army.aspx

Liebowitz, M. Estonia Forms Volunteer Cyber Army. March 14th, 2011. Retrieved from:
http://www.nbcnews.com/id/40949769/ns/technology_and_science-security/t/estonia-forms-volunteer-cyber-army/#.WXEJeVGQzIU

The Baltic Times (2011, January 11). Estonia to establish 'cyber defense league'. January 11th, 2011. Retrieved from: https://www.baltictimes.com/news/articles/27704/

9. Documents

N/A

10. Related Law / Policies / Etc.

The Estonian Defense League Act

11. Keywords

Volunteering, Cyber Defense, Emergency Response, Army Reserve

12. Snapshot

- Targeted population: Cybersecurity and IT professionals
- Geographical scope: Estonia
- Policy type: Capacity building and operation
- Statut: Active

France

Cyberdefense Citizen Reserve (CCR)

France – Cyberdefense Citizen Reserve (CCR)

1. Summary

The Cyberdefense Citizen Reserve (CCR) was created in 2012, following the publication of the Bockel report. Managed by the army, its mandate is to develop activities in order to disseminate information and raise public awareness on cybersecurity and cyberdefense issues, so that private companies and the public sector can be better protected against threats. It is made up of approximately forty citizens from the civilian workforce, organized in several working groups.
In 2016, the Operational Cyberdefense Reserve was created. It is composed of reservists who can be called upon to provide incident-response capacities in the event of a cyber-attack.

2. Nature

Public Awareness; Capacity Building.

3. Policy's Description

- **Date** :
  - 2012: Cybersecurity Citizen Reserve is created.
  - 2016: Cybersecurity Operational Reserve is created.
- **Country** : France
- **Geographical scope** : France
- **Instigator** : Ministry of Defense
- **Targeted issue / situation** :
  Lack of cybersecurity expertise to protect public and private networks and raise awareness about cyber risks.
- **Targeted population** :
  The Cyberdefense Citizen Reserve aims at increasing basic skills in cybersecurity in most public and private companies. Its goal is to develop cybersecurity knowledge and enrol volunteers for outreach activities. It also aims at developing the expertise in the fields of cybersecurity and cyberdefense.
- **Goals of the policy** :
  - The CCR aims to carry on and amplify technical and human means allocated to cyberdefense.
  - The primary goal is to develop cyberdefense spirit, bring independent thinking and influence decision makers.
  - The secondary goal is to raise awareness, explain, debate, set up events contributing to make cyberdefense a national priority.

- **Components of the policy** :
  - Volunteers: Citizens with various backgrounds, who are all either working in or showing an interest for cyberdefense and cybersecurity issues. They're organized in working groups targeting specific stakeholder groups: journalist and elected officials, millennials, citizen engagement, think tank and strategic research, small businesses, large companies.
  - Intervention type: Organization and planning of events aimed at raise awareness on cybersecurity / cyberdefense, develop expertise, build networks, information and awareness activities.
- **Agents in charge** :

1) Cyberdefense Citizens Reserve: goal is to inform and raise awareness across the nation on cyberdefense issues. Made up of volunteers linked to the army and organized in working groups on different themes.
2) Operational Cyberdefense Reserve (created in 2016): Pool of reservists that can provide operational support in case of a major cyber crisis.

- **Costs** : N/A
- **Sources of funding** : Ministry of Defense
- **Penalties** : No
- **Incentives** : No
- **Challenges** : No

4. Implementation Information

- 2012: Bockel report: recommends the creation of a citizen reserve on cyberdefense.
- 2012: Creation of the Cyberdefense Citizens Reserve (CCR), made up of volunteer civilians.
- 2013: RCC reaches up to 40 volunteers.
- 2016: Creation of the Operational Cyberdefense Reserve (OCR).
- 2017: RCC reaches up to 150 volunteers.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

http://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/bilan-et-evenements/bilan-cyberdefense-de-l-annee-2013/le-reseau-de-la-reserve-citoyenne-cyberdefense

7. Publications

N/A

8. Media Articles

Caproni, N. Coup de projecteur sur la réserve citoyenne cyberdéfense. October, 10th, 2013. Blog cyber-securité.fr.
http://www.cyber-securite.fr/2013/10/10/coup-de-projecteur-sur-la-reserve-citoyenne-cyberdefense/

9. Documents

Bockel, JM. (2012). La cyberdéfense, un enjeu mondial, une priorité nationale. *Sénat, Rapport d'information 681 de la Commission des affaires étrangères, de la défense et des forces armées*. https://www.senat.fr/notice-rapport/2011/r11-681-notice.html

Ministère de la Défense (2013). *Livre Blanc de la Défense.* Paris.
http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf

10. Related Law / Policies / Etc.

Cyberdefense reserve (RCD)

11. Keywords

Army Reserve, Awareness Activities, Incident Response

12. Snapshot

- Targeted population: Volunteers (students, cybersecurity and IT professionals)
- Geographical scope: France
- Policy type: Public Awareness, Capacity Building
- Status: Active

Germany

Anti-Botnet Advisory Centre

Germany - Anti-Botnet Advisory Centre

1. Summary

The German Anti-Botnet Advisory Centre is a private initiative led by the Association of the German Internet Industry, eco. Established in 2010, the centre collaborates with Internet Service Providers (ISPs) and various antivirus companies to inform computer users about infections on their machines and provide them with the tools necessary to treat the infection and protect themselves from future attacks. The Centre operates a service online called botfrei that offers computer security advice, resources, downloadable malware cleaning tools and a telephone hotline for more advanced support.

2. Nature

Anti-Botnet Strategy

3. Policy's Description

- **Date** : September 2010: Centre operations begin.
- **Country** : Germany
- **Geographical scope** : Germany
- **Instigator** : Eco, Germany's private internet industry association.
- **Targeted issue / situation** :
  There are millions of botnet infected computers internationally and Germany was among the top ten most malware-infected countries in the world after being severely hit by the 2009 Conficker virus.
- **Targeted population** : German ISPs, computer users.
- **Goals of the policy** :
  The centre's main goal is to reduce to amount of botnet infected machines in Germany. It aims to get the country out of the top ten most infected worldwide list.
  It also aims to decrease botnet-related crime and support internet user's sense of security online.
- **Components of the policy** :
  The German Anti-Botnet Advisory centre is an online help service that provides information on computer security and malware removal tools. The advisory operates at botfrei.de and has three parts: Inform, Clean and Prevent.
  - Inform: ISPs participating in the Botnet Advisory Centre identify network infections and

exchange information about suspected botnets with one another. They do so without resorting to deep packet inspection, therefore no personal user information is recorded. Once an infected machine is identified, the owner of the computer is notified and referred to the Anti-Botnet Advisory where they can learn more about malware infections and how to clean their computer. Curious computer users can also visit the botfrei website at any time to inform themselves about botnets, malware and general computer security.

- Clean: eco has partnered with different anti-virus companies to provide a cleaning tool called "DE-Cleaner" which detects malware and removes it. These companies include Avira, Kaspersky and Symantec. The DE-Cleaner also offer a System Recovery-CD for more heavily infected machines. There is also a telephone support hotline with a ticketing system for those requiring additional help.
- Prevent: the website provides preventative measures for the future, including general computer security tips with downloads and instructions for anti-virus scanners, firewalls, service packs and security updates.

The Germany Anti-Botnet Advisory Centre spawned the Advanced Cyber Defence Centre (ACDC). Funded by the European Innovation Framework Programme Policy Support Programme (CIP-PSP), the ACDC united 28 organizations from 14 European countries, including botfrei, to fight against botnets from 2013 to 2015. The ACDC initiative was led by eco and offered services similar to those provided by the German Anti-Botnet Advisory, but for all of Europe.

- **Agents in charge** :
  1) The Association of the German Internet industry, eco, is the exclusive project manager. Eco is the largest internet industry association in Europe and has been essential to the development of the internet in Germany.
  2) Eco works in close collaboration with the Federal Office for Information Security (BSI). This federal office is charged with managing computer and communication security for the German government. The BSI provides eco with technical support and expertise for the Anti-Botnet Advisory Centre.
- **Costs** : Start-up costs were EUR 2 million; subsequent years N/A.
- **Sources of funding** :

  Start-up funding provided by the German Ministry of the Interior. Government did not guarantee funding beyond the first year for the telephone hotline service. In 2012, eco assured the continuation of the centre for at least another year without government funding. It seems that eco has been continuously funding the program since 2013.
- **Penalties** : No
- **Incentives** : No
- **Challenges** : No

4. Implementation Information

- December 2009: Project presented by eco at IT summit.
- March 2010: Project setup commences.
- September 2010: Centre operation begin.
- January 2013: Creation of European Advanced Cyber Defence Centre (ACDC).
- July 2015: End of ACDC. Germany Anti-Botnet Advisory Centre continues.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

www.botfrei.de

7. Publications

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, Retrieved from: https://link.springer.com/article/10.1007/s10611-016-9649-z

Karge, S. (2010). The German Anti-Botnet Initiative. OECD Workshop: The role of Internet intermediaries in advancing public policy objectives. Retrieved from: https://www.oecd.org/sti/ieconomy/45509383.pdf

Kraft, T. (2012). The German anti-botnet advisory center. *ICANN 44*, 24-29, Retrieved from: https://archive.icann.org/en/meetings/prague2012/bitcache/DCIX%20Traffic%20Analysis%20%E2%80%93%20Thorsten%20Kraft,%20eco-vid=37369&disposition=attachment&op=download.pdf

The Organisation for Economic Co-operation and Development. (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD. Retrieved from: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en#page1

The Organisation for Economic Co-operation and Development. (2012). Proactive Policy Measures by Internet Service Providers against Botnets. *OECD Digital Economy Papers, 199*. Retrieved from: http://dx.doi.org/10.1787/5k98tq42t18w-en

Plohmann, D., Gerhards-Padilla, E. & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. *European Network and Information Security Agency*. Retrieved from ENISA: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

StopBadware. (2011). The State of Badware. Retrieved from: https://www.stopbadware.org/files/state-of-badware-june-2011.pdf

8. Media Articles

Cormak, A. (2012). Botnet cleanup efforts by German ISPs. June 6th. Retrieved from Jisc Community: https://community.jisc.ac.uk/blogs/regulatory-developments/article/botnet-cleanup-efforts-german-isps

9. Documents

N/A

10. Related Law / Policies / Etc.

Japan Cyber Clean Centre
Australian Internet Security Initiative
Korean Computer Emergency Response Coordination Centre
European Advanced Cyber Defence Centre

11. Keywords

Botnets, ISPs, Malware, Harm Reduction

12. Snapshot

- Targeted population: ISPs and Malware-infected computer users
- Geographical scope: Germany
- Policy type: Anti-Botnet Strategy
- Status: Active

Israel

CyberSpark / Cyber Innovation Arena

Israel – CyberSpark / Cyber Innovation Arena

1. Summary

CyberSpark is a programme aimed at developing a cyber-city in the Beer-Sheva municipality. Companies, academia, government agencies and militaries from all over the world are welcomed to work together to develop a new generation of experts and create new opportunities in the cyber security industry.

2. Nature

R&D & Economic Development

3. Policy's Description

- **Date** : January 2014: Launch of CyberSpark.
- **Country** : Israel
- **Geographical scope** : Israel; International
- **Instigator** :
  The Israel National Cyber Bureau, of the Prime Minister's Office. The Bureau's mandate is to advance defense and build national strength in cyber security, build the country's lead in the cyber field, and advance processes that support those two previous objectives.
- **Targeted issue / situation** :
  Need to develop Israel's cyber defence capabilities and raise awareness regarding cybersecurity challenges in the country, since Israel has attracted 10% of all global investment in cybersecurity R&D.
- **Targeted population** : Cyber industry and investors worldwide.
- **Goals of the policy** :
  Creating an international cyber ecosystem, where industries of all sizes (start-ups to multinationals), academia, military and government can cooperate to develop the next generation of cyber experts and companies.
- **Components of the policy** :
  CyberSpark offers many platforms to assist cyber businesses such as:
  - Research center: in collaboration with Ben Gurion University of the Negev (BGU);
  - R&D hub: supported by the Israeli government, and allows businesses to bid for potential contracts and do research with BGU;
  - Training Center: services offered to industry and SMEs;
  - Innovation Hub: exposure to Israel's innovative and advanced technologies;

- Incubator: with the support of the Israel Innovation Authority;
- Intelligence Center: Israel's CERT and companies provide intelligence relating to imminent cyber threats.

Businesses can join their affiliate club and have:
- Exclusive access to stakeholders and expertise;
- Invitations to events and workshops;
- Access to all CyberSpark's visitors and have an opportunity to network;
- Access to e-Newsletter.

A number of international agreements were signed by CyberSpark with:
- Masstech (Massachusetts);
- The State of Rhode Island;
- Ludwig Bolkow Campus, Munich;
- The University of New Brunswick

A partnership was also announced between the UK Israel Tech Hub at the British Embassy in Israel and CyberSpark.

- **Agents in charge** :

1) Joint project between the Israeli National Cyber Bureau (of the Prime Minister's office), Beer-Sheva municipality, Ben Gurion University (BGU) and leaders in the cybersecurity industry;
2) Founders and current tenants (as of 2016), and who are for the most part private companies: Oracle, Wix, leidos, DELL EMC, dbMotion, IBM, CoroNet, SCADAfence, Mellanox Technologies, Allscripts, OneHour Translation, JVP Cyber Labs (Jerusalem Venture Partners), Secret Double Octopus, AudioCodes, CyActive, SecBI, MorphiSec, BGN, PayPal, Dalet, CDI Negev, Deutsche Telekom Laboratories, CERT-IL, Elbit Systems, incubit technology ventures, L7 Defense, RAD;
3) Multinationals like Deutsche Telekom, PayPal, Oracle, Lockheed Martin, EMC and IBM can be found in the CyberSpark complex. Also, the Israeli cyber branch of the military, "Unit 8200", will be present, as well as the security agency Shin Bet and Israel's CERT;
4) Research partnership with University of New Brunswick in Canada and cooperation with MassTech.

- **Costs** : Unknown
- **Sources of funding** :

Governmental funding for the research center and for Cyber educational programs in Beer-Sheva.

- **Penalties** : No
- **Incentives** :

Companies that relocate in Israel receive grants under the form of salary subsidies that can

reach up to 40%. Companies that keep intellectual property in the country may receive other credits and deductions.

- **Challenges** : No

4. Implementation Information

January 2014: Launch of the CyberSpark program.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

http://cyberspark.org.il/

7. Publications

Getz, D., Goldberg, I., Shein, E., Eidelman, B., & Barzani, El. (2016). Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel. *World Bank Development Report 2016*, 1-92. Available at: http://pubdocs.worldbank.org/en/868791452529898941/WDR16-BP-ICT-Sector-Innovation-Israel-Getz.pdf

Zehavi, R. (2016). Transforming a Desert City into an International Cybersecurity Hub and Ecosystem. *Technology Innovation Management Review, 6*(4), 44-45. Available at: http://www.elexpro.ru/TIMReview_April2016.pdf#page=43

8. Media Articles

Ben-Gurion University of the Negev. CyberSpark – The Israeli Cyber Innovation Arena. 2016. Retrieved from: http://in.bgu.ac.il/en/cyber/Pages/Innovation-Arena.aspx

CyberSpark. CyberSpark Newsletter. March 2017. Retrieved from: http://members.viplus.com/view.ashx?message=e42059238O103533970O172260O103491238&r=1

CyberSpark. CyberSpark Newsletter. June 2017. Retrieved from: http://members.viplus.com/view.ashx?message=e42051149O103525945O172260O103499021&r=1

Stuart, H. Cybersecurity is being written in the Israeli Desert. February 1st, 2016. Retrieved from: https://motherboard.vice.com/en_us/article/d7yvay/the-future-of-cybersecurity-is-being-written-in-the-israeli-desert

University of New Brunswick. UNB forges partnership with Israeli cybersecurity initiative, marking a first. May 15th, 2017. Retrieved from: https://blogs.unb.ca/newsroom/2017/05/15/unb-forges-partnership-with-israeli-cybersecurity-initiative-marking-a-first/

Governor of Massachusetts. Massachusetts & Israeli Organizations Sign Cybersecurity Agreement. December 11th, 2016. Retrieved from: http://www.mass.gov/governor/press-office/press-releases/fy2017/ma-israeli-organizations-sign-cybersecurity-agreement.html

Nakashima, El. & Booth, W. How Israel is turning part of the Negev Desert into a cyber-city. May 14th, 2016. Retrieved from: https://www.washingtonpost.com/world/national-security/how-israel-is-turning-part-of-the-negev-desert-into-a-cyber-city/2016/05/14/f44ea8e4-0d58-11e6-bfa1-4efa856caf2a_story.html

Zehavi, R. How Israel is carving out a corner of the cyber-security market. April 3rd, 2016. Retrieved from: http://ipolitics.ca/2016/04/03/how-israel-is-carving-out-a-corner-of-the-cyber-security-market/

Press, V. S. Beersheva goes cyber. August 3rd, 2015. Retrieved from: https://www.israel21c.org/beersheva-goes-cyber/

9. Documents

N/A

10. Related Law / Policies / Etc.

Resolution No. 3611, of the Israel National Cyber Bureau, available at: http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx.

11. Keywords

R&D, Economic Development, Public-Private Partnership

12. Snapshot

- Targeted population: Cybersecurity industry and investors
- Geographical scope: Israel, international
- Policy type: R&D & Economic Development
- Status: Active

Japan

Cyber Clean Center

Japan – Cyber Clean Center

1. Summary

The Cyber Clean Center was a 5-year cleaning operation led by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry in Japan. This operation consisted in detecting bot-infected computers in Japan, collecting data on the detected bot malwares and creating bot-removal tools and sending them by email to all concerned users. This program was led in cooperation with numerous Internet Services Providers (ISP) and security vendors. By the end of the 5-year operation, the rate of infected computers dropped from 2.5% to 1%.

2. Nature

Anti-Botnet Strategy

3. Policy's Description

- **Date** :
  - December 2006: Beginning of the program.
  - March 2011: End of program.
- **Country** : Japan
- **Geographical scope** : Japan
- **Instigator** :
  Japanese government. The CCC was led by the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI).
- **Targeted issue / situation** :
  Botnet infections are rising, and there are more and more subspecies of bots. Furthermore, they are difficult to remove from users' computers.
- **Targeted population** : End-users infected by malware.
- **Goals of the policy** :
  The main goal is to reduce botnet infections as close to zero as possible, to create botnet removal tools and to provide malware specimen to security vendors participating in the program.
- **Components of the policy** :
  The CCC analyses botnets' characteristics and provides information regarding their removal from user's computers.

Steps of their activities:

1. Detection of botnet infections and capture of bot samples.
2. Request of identification of the infected computers in collaboration with ISPs (Internet service providers).
3. Preparation and creation of bot removal tools by security vendors.
4. The ISPs detect the infected computers.
5. The ISPs send their users alerts of infection by email.
6. In the email, the users can access a countermeasures website and remove the malicious software.

- **Agents in charge** :

Within the CCC, there are different groups:

1) The Cyber Clean Center Steering Committee: reviews policies and activities of the CCC. Led by the MIC and METI.
2) Bot Countermeasure System Operation Group: locates botnet-infected computers and notifies users about the possible countermeasures. The group is led by Telecom-ISAC Japan, in collaboration with ISPs.
3) Bot Program Analysis Group: analyses the characteristics and technical elements of the botnets, develops countermeasure tools based on those analyses. Led by JPCERT Coordination Center and Trend Micro in cooperation with security vendors.
4) Bot Infection Prevention Promotion Group: enhances botnet infection prevention measures and re-infection prevention for users. Led by Information-technology Promotion Agency Japan (IPA) in collaboration of security vendors.

The CCC works in collaboration with 76 Internet Service Providers, one disinfection tool developing company (Trend Micro) and seven security vendors.

- **Costs** : Unknown
- **Sources of funding** : Governmental, Funded by the METI and MIC.
- **Penalties** : No
- **Incentives** : Free malware removal tools distributed to infected users.
- **Challenges** : No

4. Implementation Information

- December 2006: launch of the project.
- 2009: review of the operation, and development of a new honeypot system.
- March 2011: end of the project.

5. Evaluation

- **Existence of an evaluation** : Yes
- **Evaluation type** :
  Self-reporting of outputs and outcomes (Annual report of the CCC, August 2010).
- **Evaluator** : The CCC
- **Methodology** : Unknown
- **Outcomes** :
  - Total cumulative number of malware samples collected was 16 million (1 million of malware types). From these 30,000 unknown malware samples were obtained;
  - ISPs sent approximately 480,000 e-mails to 100,000 users;
  - 31.6% of the warned users downloaded the CCC suggested countermeasures. On their website, the CCC Cleaner was downloaded more than 1.2 million times. The installation rate and percentage of successful disinfections remain unknown;
  - Since 2009, a decrease in detecting malware was observed;
  - The infection rate of users in Japan decreased from 2-2.5% in 2005 to 1% in 2008. The project was effective, but with the combined impact of the production of more secure PCs' operating systems from tech companies.

6. URL

https://www.telecom-isac.jp/ccc/en_index.html

7. Publications

Komatsu A., Takagi D., Takemura T. (2013). Human aspects of information security − An empirical study of intentional versus actual behaviour. *Information Management & Computer Security, 21*(1), 5-15. Available at: http://www.emeraldinsight.com/doi/full/10.1108/09685221311314383

Ito, Y. (2011, June). Making the Internet clean, safe and reliable: Asia Pacific regional collaboration activities. In *Cybersecurity Summit (WCS), 2011 Second Worldwide* (pp. 1-3). IEEE. Available at: http://ieeexplore.ieee.org/document/5978796/

Yamada, Y., Yamagishi, A., & Katsumi, B. T. (2010). A Comparative Study of the Information Security Policies of Japan and the United States. *Journal of National Security Law & Policy*, *4*(217), 217-232. Available at: http://jnslp.com/2010/09/29/a-comparative-study-of-the-information-security-policies-of-japan-and-the-united-states/

Takemura, T., & Umino, A. (2009). A quantitative study on Japanese Internet users' awareness to information security: necessity and importance of education and policy. *World Academy of Science, Engineering and Technology, 60*, 638-644. Available at: https://waset.org/Publication/a-quantitative-study-on-japanese-internet-user-s-awareness-to-information-security-necessity-and-importance-of-education-and-policy/11876

8. Media Articles

Krebs, B. Talking Bots with Japan's 'Cyber Clean Center'. March 1st, 2010. Retrieved from: https://krebsonsecurity.com/2010/03/talking-bots-with-japans-cyber-clean-center/#more-896

9. Documents

N/A

10. Related Law / Policies / Etc.

N/A

11. Keywords

Anti-Botnet, Harm Reduction Strategies, Honeypots, ISPs, Public-Private Partnership

12. Snapshot

- Targeted population: ISPs, Individual users
- Geographical scope: Japan
- Policy type: Anti-Botnet Strategy
- Status: Inactive

Korea

1) Korea Computer Emergency Response Team Coordination Center (KrCERT/CC)
2) Personal Information Protection Act (PIPA)

Korea – Korea Computer Emergency Response Team Coordination Center (KrCERT/CC)

1. Summary

The Korea Computer Emergency Response Team Coordination Center (KrCERT/CC) is a federal cybersecurity center that aims to protect private organizations from an increasing number of cyber-attacks. In collaboration with Korean Internet Service Providers (ISPs), KrCERT operates a Domain Name Service (DNS) sinkhole program that redirects traffic from malicious hosts to a secure server. It also provides different forms of technical advice and solutions to users who may be concerned by malware, such as cybersecurity drills, online services and a help-desk. The KrCERT participates in constant network monitoring to gather malware information to service its programs and shares its findings internationally.

2. Nature

Anti-Botnet Strategy

3. Policy's Description

- **Date** :
  A computer response team was established in 2005 and became formally recognized as KrCERT in 2010.
- **Country** : South Korea
- **Geographical scope** : South Korea
- **Instigator** :
  Korea Information Security Agency, now known as the Korea Internet & Security Agency (KISA).
- **Targeted issue / situation** : Increasing number of cyber-attacks from North Korea and elsewhere.
- **Targeted population** :
  Private organizations in South Korea and their computer and network systems, Korean Internet Service Providers.
- **Goals of the policy** : Respond to computer network security incidents.
- **Components of the policy** :
  - KrCERT collaborates with Internet Service Providers (ISPs) to protect computer users from various infections. It performs real-time non-stop network monitoring and continuously gathers information on botnet-infected machines, malware-infected websites and malicious control-and-command servers. Using this information, KrCERT operates a Domain Name

Service (DNS) sinkhole program that blocks the infected machines from communicating with botnet command centers. With the collaboration of ISPs, the sinkhole redirects traffic from malicious domains to a safe server run by KISA. The information retrieved from the DNS sinkhole scheme is then used in a database for KrCERT's online bot-infection checking service. This service runs as a website that concerned computer users can visit if they believe their machines is infected by a botnet. KISA also operates a help-desk service through KrCERT. Computer users may call or visit the help-desk service online and are provided with remote assistance for various malware-related computer issues. KrCERT also organizes cybersecurity drills so organizations can test for vulnerabilities in their systems and develop efficient and effective responses to potential cyber-threats.

- KISA runs the 'ZombiePC Curing System', a quarantine service for infected computers: if a machine is found to be infected while active on the web, participating ISPs will quarantine the subscriber's computer and provide malware removal tools and assistance.
- KrCERT participates in international efforts to aid global cybersecurity. It is a member of the Forum of Incident Response and Security Teams (FIRST) and exchanges information with domestic and foreign cooperative systems through the Consortium of Computer Emergency Response Teams (CONCERT).

- **Agents in charge** :

1) The Korea Information Security Agency, which was established in 1996. The Agency has since been integrated into the Korea Internet & Security Agency (KISA) in 2009, created under Art under Article 52 of the Act for the Promotion of Information and Communications Use and the Protection of Information. KISA operates under the Government Ministry of Science and ICT (MSIT). Amongst other responsibilities, KISA is charged with ensuring Internet safety in Korea and cyber-attack prevention. To do so, KISA operates the Korean Internet Security Center (KISC). KISC was established in 2003 after a major malware incident.
2) The KrCERT is operates as part of and is located within KISA. It seems that KrCERT functions as a subdivision of the KISC under KISA.

- **Costs** : N/A
- **Sources of funding** : N/A
- **Penalties** : No
- **Incentives** : No
- **Challenges** : N/A

4. Implementation Information

- 2004: Computer emergency response team established.

- 2005: DNS Sinkhole scheme launched.
- 2010: Quarantine service launched.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.krcert.or.kr/krcert/intro.do

7. Publications

Carr, J. (2009). *Inside Cyber Warfare: Mapping the Cyber Underworld* (1st ed.). O'Reilly Media, Inc.

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, Retrieved from: https://link.springer.com/article/10.1007/s10611-016-9649-z

The Organization for Economic Co-operation and Development. (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives.* OECD. Retrieved from: http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en#page1

8. Media Articles

Jung, M. S. How to organize a national cybersecurity drill. March 28th, 2017. Retrieved from APNIC: https://blog.apnic.net/2017/03/28/organize-national-cybersecurity-drill/

9. Documents

N/A

10. Related Law / Policies / Etc.

Japan Cyber Clean Centre

Australian Internet Security Initiative

German Anti-Botnet Advisory Center

11. Keywords

Botnet, CERT, Incident Response, Malware, Public-Private Partnership

12. Snapshot

- Targeted population: Private organizations
- Geographical scope: South Korea
- Policy type: Anti-Botnet Strategy
- Status: Active

Korea – Personal Information Protection Act (PIPA)

1. Summary

The Personal Information Protection Act (PIPA) of South Korea is a law that emphasizes the importance of informed consent when processing personal data. PIPA requires all organizations interested in using personal information from an individual to obtain informed consent from said individual before processing their personal information. Organizations must also ensure the physical and digital protection of personal information in their possession and must comply if asked to withdraw or destroy the data. Organizations found in violation of PIPA may face civil or criminal charges.

2. Nature

Privacy Protection

3. Policy's Description

- **Date** :
  - March 2011: Law enacted.
  - September 2011: Law effective.
- **Country** : South Korea
- **Geographical scope** : South Korea
- **Instigator** : Korean government
- **Targeted issue / situation** :
  There are more and more reports of large-scale personal data leakages involving different corporations, organizations and institutions in South Korea. Often, these leaks are a result of internal misconduct or negligence. The Constitutional Court of South Korea recognizes data privacy as a fundamental right under the broader constitutional right to privacy. Personal data leaks can harm and result in fraud of the affected individuals.
- **Targeted population** :
  Public and private South Korean organizations and institutions that process personal information, Citizens.
- **Goals of the policy** :
  PIPA was conceived to uphold the right to privacy by strengthening the protection of personal information in Korea. It aims to ensure the individual agency of citizens over their personal information by bringing transparency to data collection processes and holding data collectors accountable for harvesting personal information without consent.

- **Components of the policy** :
  - PIPA requires that all data processors obtain the informed consent of individuals before processing personal information. Data processors also have an obligation to collect the minimum amount of personal information necessary to provide their service and to handle personal information anonymously whenever possible.
  - When the data processor obtains consent, it must inform the individual of the purpose of collection of personal information, the type of personal information to be collected, the period of time in which the personal information will be stored and that consent may be refused. Data collectors must take measures to secure the physical and digital safety of personal information. Sensitive personal information and unique identifiers require separate consent from individuals and must remain encrypted and more closely safeguarded. In order to transfer personal information to a third party, data processors must obtain separate consent from individuals. If this transfer is expected to be cross-border, separate consent is also required.
  - Individuals retain certain control rights over their information even after granting consent. If they make a request to alter or stop further processing of the information provided, the data processor must comply.
  - If someone feels their rights have been violated or need more information about PIPA, they may contact the Personal Data Infringement Call Center. The Center receives, investigates and addresses all types of data-related privacy complaints and questions. It may transfer cases of lesser misconduct to the Personal Data Dispute Mediation Committee, which is an alternative dispute resolution organization. The Committee mediates disputes between individuals and processors in an amicable fashion and recommends civil compensations. If the case is found to be a more serious violation, it is transferred to the Minister of the Interior and Safety for a criminal procedure.
- **Agents in charge** :

  Ministry of the Interior and Safety (MOIS):
  - Known as the competent authority of the Personal Information Protection Act, the MOIS is responsible for developing and enforcing the PIPA and other data-based legislation. They investigate the handling of personal information and impose sanctions when PIPA is found to be violated.

  Personal Information Protection Commission (PIPC):
  - An independent body established under PIPA to protect individual privacy rights. The PIPC deliberates on and resolves personal data-related policies and mediates opinion differences between government agencies. It does not resolve individual data complaints – this is left to the MOSI.

Personal Data Infringement Call Center:

- Established by the MOIS, it is tasked with receiving calls from individuals with data privacy-related concerns or complaints. Employees at the Call Center will give counsel and information to those needed and are charged with investigating complaints and transferring cases to the appropriate authorities.

Personal Data Dispute Mediation Committee:

- Composed of public officials, professors, researchers or other recognized individuals specialized in data protection, this committee serves to resolve personal data disputes. It is tasked with settling these disputes by ordering a suspension of the violation activities, restitutions or damages to be paid to the victim or any other civil measure found to be effective in mediating the dispute. If the dispute is found to compose criminal charges, the case is transferred to the MOIS for a proper criminal procedure.

- **Cost** : N/A
- **Sources of funding** : N/A
- **Penalties** :

  Depending on the nature of the infraction, civil or criminal penalties may apply. Civil penalties may occur after successful mediation and may include various forms of compensation found acceptable by both parties during the mediation process or a civil suit. These may include financial compensation, administrative measures, fines and sanctions or advice improvements. For example, the mishandling of resident registration numbers may include a fine up to approximately USD 441,000 (500 million won). Criminal penalties include imprisonment up to 10 years or a fine up to approximately USD 88,000 (100 million won).

- **Incentives** : N/A
- **Challenges** : N/A

4. Implementation Information

- March 2011: Law promulgated.
- September 2011: Law effective.
- March 2012: Grace period for companies to comply with the PIPA ends.
- March 2013; August 2013; March 2014; November 2014; July 2015; March 2016; and April 2017: Various amendments such as notifications for third-party data transfers, security measures for sensitive information and regular inspection on unique identifier encryption.

5. Evaluation

- **Existence of an evaluation** : Yes

- **Evaluation type** :
  1) Draft Paper.
  2) Ko, H., Leitner, J. M., Kim, E., & Jung, J.-G. (2017). Structure and Enforcement of Data Privacy Law in South Korea. *SSRN Scholarly Paper No. ID 2904896*. Available at SSRN: https://papers.ssrn.com/abstract=2904896
- **Evaluator** :
  1) Haksoo Ko is Professor at Seoul National University (SNU) School of Law, Seoul, Korea.
  2) John Leitner is Visiting Researcher at SNU School of Law and law clerk for the United States District Court for the District of Maine and Executive Committee member.
  3) Eunsoo Kim and Jong-Gu Chung are doctoral candidates at SNU School of Law.
- **Methodology** : Legal analysis
- **Outcomes** :

  Recent legal developments suggest that informed consent is only legally effective if individuals have a very clear understanding of the information being used and the implications of their consent. PIPA's approach has not yet shown to be effective. Though it may limit the number of new data-based industries, it may not adequately protect individual personal information.

6. URL

https://www.privacy.go.kr/eng/

7. Publications

Lee, E., & Kim, D. (2016). A Study on the Framework Changes of Personal Information Protection in Korea. *International Journal of Software Engineering and Its Applications, 10*(7), 1–10. https://doi.org/10.14257/ijseia.2016.10.7.01

8. Media Articles

Hee-Eun, K. Korea Strengthens Protection for "Resident Registration Numbers" (RRNs): Leaks May Face a Fine of up to 0.5 Billion Korean Won. August 7th, 2013. Retrieved from https://www.insideprivacy.com/international/korea-strengthens-protection-for-resident-registration-numbers-rrns-leaks-may-face-a-fine-of-up-to-0-5-billion-korean-won/

Iqbal, S. Grace Period for Compliance with New Korean Privacy Law Ended this Spring. July 3rd, 2012. Retrieved from https://www.insideprivacy.com/data-security/grace-period-for-compliance-with-new-korean-privacy-law-ended-this-spring-1/

Kang, T. U. 2016 Spring Data Protection and Privacy News Alert. April 26th, 2016. Retrieved from

https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/05/bkl-Legalupdate-20160426_v2.pdf

Ramirez, E., & Lynch, G. South Korea Joins Asia-Pacific Data Transfer System. June 28th, 2017. Retrieved from https://www.bna.com/south-korea-joins-n73014460915/

9. Documents

https://www.privacy.go.kr/eng/remedy_01.do
https://www.privacy.go.kr/eng/remedy_02.do

10. Related Law / Policies / Etc.

Act on the Promotion of Information and Communications Network Utilization and Information Protection (South Korea)
Use and Protection of Credit Information Act (South Korea)
Use and Protection of Location Information Act (South Korea)
Communications Secrecy Act (South Korea)

11. Keywords

Personal Information, Data Protection, Informed Consent.

12. Snapshot

- Targeted population: Citizens and institutions
- Geographical scope: South Korea
- Policy type: Privacy protection
- Status : Active

Netherlands

1) AbuseHUB
2) Dutch Anti-Botnet Initiative
3) Hague Security Delta (HSD)
4) SME Cybersecure, Cybersecurity Business Edition

Netherlands – AbuseHUB

1. Summary

The Abuse Information Exchange Team is in charge of the AbuseHUB platform, which collects and analyses data regarding botnet infections and sends information to the relevant Internet Service Providers (ISPs). In turn, they contact their customers in case of an infection. This Dutch initiative was launched with the collaboration of ISPs and other relevant stakeholders to protect end-users in the Netherlands. This project follows the Dutch Anti-Botnet Initiative that was initiated in 2009.

2. Nature

Anti-Botnet Strategy

3. Policy's Description

- **Date** :
  - June 2014: AbuseHUB becomes operational.
- **Country** : Netherlands
- **Geographical scope** : Netherlands
- **Instigator** : A collective of private companies and ISPs.
- **Targeted issue / situation** :
  Research suggests that 5 to 10% of computer users are infected by botnets every year in the Netherlands.
- **Targeted population** : ISPs and ultimately, end-users.
- **Goals of the policy** :
  - Exchange of information regarding botnet infections and other internet abuse by: collecting, analysing and correlating information from various resources.
  - Identifying and mitigating risks for end-users, and facilitating effective countermeasures.
- **Components of the policy** :
  The sharing platform, managed by the Abuse Information Exchange Team, collates, analyses and sorts botnet infection reports, before sending them to the relevant ISPs. Then, once the latter have a report of the situation, they can work with their customers and deal with the infections. More precisely:
  - AbuseHUB gets its information from various Dutch and international entities. Those sources are known as 'reliable notifiers' because they have to be screened prior to becoming an

information provider. Only companies with registered IP-space and an abuse policy that gives them the responsibility to act on the information received can be part of the abuse association.

  - ○ Some notifiers are: Team Cymru, ReturnPath, Aol, Windows, SpamHaus, Politie, National Cyber Security Center for the Ministry of Security and Justice, ACDC, Autoriteit Consument & Markt.

- Reports from the reliable notifiers are then analysed and sent to the related ISPs so they can take action.
- AbuseHUB is also a forum for members to share their expertise and work together to make the internet safer.

- **Agents in charge** :
  1) AbuseHUB is an initiative by the Abuse Information Exchange, where Dutch ISPs and stakeholders collaborate. Members include KPN (Dutch Telecom and IT service provider), RoutIT, SIDN Labs (Dutch internet domain registrar), Solcon, SURFnet, Tele2, UPC (United Philips Cable), XS4ALL, ZeelandNet and Ziggo.
  2) This initiative is run by private companies, who are collectively responsible for more than 95% of internet connections in the country, and more than 70% of domains ending in ".nl".
- **Costs** : N/A
- **Sources of funding** :
  Financial support from the Dutch Ministry of Economic Affairs and SIDN (Dutch internet domain registrar).
- **Penalties** : No
- **Incentives** :
  The opportunity to self-regulate is seen by the private sector as preferable to more coercive state regulation.
- **Challenges** : No

4. Implementation Information

- 2012: Creation of the Abuse Information Exchange team.
- November 2013: launch of project prototype.
- January 2014: Pilot phase of the project, led by ISPConnect, DHPA (Dutch Hosting Provider Association) and AbuseIX.
- June 2014: official launch of the operation.

5. Evaluation

- **Existence of an evaluation** : Yes
- **Evaluation type** :
  1. Report from the initiative.
  2. Empirical evaluation.
- **Evaluator** :
  1. Abuse Information Exchange.
  2. Report commissioned by the Ministry of Economic Affairs, produced by Moura, Lone, Asghari and van Eeten.
- **Methodology** :
  1. Unknown.
  2. Evaluation of the infection rates of Dutch ISPs over different time frames. Three data sources cover January 2011 to December 2014, and other sources cover parts of 2014. These sources can be ISPs, sinkholes, botnets, spam traps and feeds from the Shadowserver Foundation. Data was collected both externally (identifying infected machines by their behaviors) and internally from botnets (through interception of communication between bots and their Command & Control Centre).
- **Outcomes** :
  1. In September 2014:
     - Already 4.7 million abuse reports received and processed.
     - 100 abuse types identified.
     - Reports were sorted, distributed and covered 35 Autonomous System Numbers (ASN) in total.
  2. The Netherlands performs relatively well in terms of botnet mitigation when compared to other countries in the world:
     - Since 2011, most reference countries have improved over time. But the infection rates in the Netherlands are relatively low when compared to the other countries observed. There have also been faster clean ups for spam and botnets (Conficker related);
     - Dutch ISPs perform well in comparison with other ISPs from different countries. Countries with mature anti-botnet initiative like the Netherlands have also lower infection rates per subscribers. But there are also countries with no anti-botnet initiative that also have lower infection rates than some countries with such initiatives. This means that the existence of this type of initiative doesn't dictates how well ISPs perform;
     - The Netherlands performs substantially well when compared to the other 60 countries. Their ranking also remains stable between 2009 and 2014;
     - The majority of infected machines in the Netherlands are from the AbuseHUB member networks, but it is because these ISPs cover most of the IP addresses in country. Also,

AbuseHUB members are improving more than non-members overtime;

- It is not possible at this stage to conclude about the impact of AbuseHUB in botnet mitigation in the country since it only started operations in 2014. But overall, there was already some progress even before the launch of AbuseHUB.

6. URL

https://www.abuseinformationexchange.nl/english

7. Publications

van Eeten, M., Lone, Q., Moura, G., Asghari, H., & Korczyński, M. (2016). Evaluating the Impact of AbuseHUB on Botnet Mitigation. pp 1-43. Available at: https://arxiv.org/abs/1612.03101

8. Media Articles

SIDN. ISP's SURFnet and SIDN ready for the war against botnets. June 6th, 2014. Retrieved from: https://www-a.sidn.nl/a/internet-security/internet-service-providers-surfnet-and-sidn-ready-for-the-war-against-botnets?language_id=2&langcheck=true

Nationaal Cyber Security Centrum. Gert Wabeke. 2014. Retrieved from: https://www.ncsc.nl/conference/conference-2014/speakers/gert-wabeke.html

Davids, M. ENTRADA link for AbuseHUB. September 3rd, 2015. Retrieved from: https://www.sidnlabs.nl/a/weblog/entrada-link-for-abusehub?language_id=2&langcheck=true

Domainnews. SIDN, ISPs & SURFnet Launch AbuseHUB to Tackle Botnets. 2015. Retrieved from: http://www.domainnews.com/sidn-isps-surfnet-launch-abusehub-to-tackle-botnets/

Wabeke, G. AbuseHUB: a Success Story. October 28th, 2014. Retrieved from: https://www.slideshare.net/splend/holland-strikes-back-gert-wabeke-abusehub

Kepinski, W. Pilot phase from AbuseHUB starts. January 4th, 2016. Retrieved from: https://translate.google.ca/translate?hl=en&sl=nl&u=https://executive-people.nl/549781/pilotfase-van-abusehub-gaat-van-start.html&prev=search

Molenaar, K. AbuseHub. March 31st, 2016. Retrieved from: https://translate.google.ca/translate?hl=en&sl=nl&u=https://www.ispconnect.nl/tag/abusehub/&prev=search

Dutch IT-channel. AbuseHUB gives hosters a complete picture of abuse from their network. February 7th, 2016. Retrieved from: https://translate.google.ca/translate?hl=en&sl=nl&u=https://dutchitchannel.nl/556652/abusehub-geeft-hosters-een-volledig-beeld-van-abuse-vanaf-hun-netwerk.html&prev=search

9. Documents

N/A

10. Related Law / Policies / Etc.

Spin-off of ECP – Platform for the Information Society, an independent platform for collaboration between government, business and social organizations that foster knowledge exchanges about the impact and responsible application of new technologies in Dutch society.
Anti-Botnet Working Group.

11. Keywords

Anti-botnet, Botnet Mitigation, Information Sharing

12. Snapshot

- Targeted population: ISPs and end users
- Geographical scope: The Netherlands
- Policy type: Anti-Botnet strategy
- Status: Active

Netherlands – Dutch Anti-Botnet Initiative

1. Summary

The Dutch Anti-Botnet Initiative aimed to fight botnet infection in the Netherlands, with the participation of fourteen different Internet Service Providers (ISPs) covering over 90% of internet access in the country. The participating ISPs' objectives were to contact their customers when infections were detected. The preliminary evaluation of the program was not very positive. A newer version of this program was launched in 2014.

2. Nature

Anti-Botnet Strategy

3. Policy's Description

- **Date** : 2009
- **Country** : Netherlands
- **Geographical scope** : Netherlands
- **Instigator** : Dutch Telecom Regulatory Authority (OPTA)
- **Targeted issue / situation** :
  End users such as home users and small and medium sized enterprises are the main victims exposed to online harms as they lack the capacities to protect their machines against cyber threats. Their computers are therefore more vulnerable to be recruited into botnets.
- **Targeted population** : ISPs and end users.
- **Goals of the policy** : The main objective of this initiative was to fight botnet infection.
- **Components of the policy** :
  This program is the collaborative effort of fourteen Internet Service Providers (ISPs), in charge of:
  - Exchanging relevant information among them. This will lead to a faster response time to deal with malware infection.
  - Putting infected machines in quarantine, to ensure that infected computers can no longer infect other machines or participate in criminal activities.
  - Notifying end-users. The relevant ISPs will have to contact the owners of the infected machines so they can take action.

  Each of the participating ISP is in charge of covering the costs of such procedures, whether it's for monitoring suspicious activities, notifying their customers or offering remediation activities.

- **Agents in charge** :
  Fourteen Dutch ISPs participated in a joint effort to fight botnet infections in an Anti-Botnet Working Group. These ISPs covered over 90% of the broadband market in the country.
- **Costs** : Costs were borne by participating ISPs.
- **Sources of funding** : Unknown
- **Penalties** : No
- **Incentives** :
  If most of the ISPs participate in this program, they won't risk losing customers, since other providers will be using the same procedures with infected computers.
- **Challenges** : No

4. Implementation Information

- 2009: beginning of the initiative.
- January 2011: Publication of program evaluation.
- June 2014: Beginning of AbuseHUB operations, the newer version of this initiative.

5. Evaluation

- **Existence of an evaluation** : Yes
- **Evaluation type** : Independent empirical evaluation
- **Evaluator** :
  Researchers commissioned by the Dutch Ministry of Economic Affairs, Agriculture and Innovation.
- **Methodology** :
  Data collected from ten different ISPs from January 2009 to June 2010.
  This study used three different data sets:
  - Spam Dataset: with spam traps and honey pots;
  - DShield Dataset: data collected by volunteers who monitor malicious online activities;
  - Conficker Dataset: provided by the Conficker Working Group, who run sinkholes for Conficker bot-infected machines.
- **Outcomes** :
  - Between January 2009 and June 2010, around 450-900,000 of infected machines were detected within the ISPs used in this study. It means that between 5-10% of all Dutch broadband users suffered an infection in 2009 and 2010.
  - During the study period, ISPs have not changed their policies drastically, or at least not

enough to see changes in infection trends. However, the analysis showed that there were, in a daily average, more infected IP addresses active in 2010 than in 2009. The overall situation in the Netherlands was worse in 2010 than in 2009, but it seems to have been caused by attackers and not because of the ISPs' initiative.

- ISPs contact approximately 10% of their infected customers. To explain this discrepancy between the number of infections and customers contacted, ISPs explained that they usually waited to find corroborating evidence before contacting the customers in case of false positives. Also, customer support is costly, which is why ISPs' performance in botnet mitigation was disappointing.

6. URL

N/A

7. Publications

van Eeten, M., Asghari, H., Bauer, J. M., & Tabatabaie, S. (2011). Internet service providers and botnet mitigation: A fact-finding study on the Dutch market. *Delft University of Technology*, 1-45.

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, Retrieved from: https://link.springer.com/article/10.1007/s10611-016-9649-z

8. Media Articles

Evron, G. Dutch ISPs Sign Anti-Botnet Treaty. September 29th, 2009. Retrieved from: https://www.darkreading.com/risk/dutch-isps-sign-anti-botnet-treaty/d/d-id/1132035

9. Documents

N/A

10. Related Law / Policies / Etc.

Platform Internet Security ("Platform Internetveiligheid").
Project Taurus of the Dutch National Police Agency.
Abuse.IX, AbuseHUB, Abuse Exchange Information.

11. Keywords

ISPs, Botnets, Botnet Mitigation, Information Sharing

12. Snapshot

- Targeted population: ISPs, end users
- Geographical scope: The Netherlands
- Policy type: Anti-Botnet Strategy
- Status: Inactive

Netherlands – Hague Security Delta (HSD)

1. Summary

The Hague Security Delta (HSD) is a leading European security cluster that was established in partnership with companies, organisations, research institutions and academia, to encourage knowledge development, job stimulation and security promotion in the following fields: national, cyber and urban security, forensics, and critical infrastructures.

2. Nature

R&D & Economic Development

3. Policy's Description

- **Date** : November 2010: initiation of the program.
- **Country** : Netherlands
- **Geographical scope** : Netherlands
- **Instigator** : The Municipality of The Hague and the Dutch Ministry of Economic Affairs.
- **Targeted issue / situation** :
  Knowledge and innovation are the necessary components of a thriving cybersecurity industry. The creation of a security cluster in the Hague is also an opportunity to enhance economic prosperity.
- **Targeted population** : Dutch and international companies, investors and students.
- **Goals of the policy** :
  "The objective is the development and stimulation of business activity, more job opportunities and the promotion of a secure world" (HSD, 2017).
- **Components of the policy** :
  One of the main concerns for HSD is to encourage the development of the economy in the Hague, by increasing the number of jobs and attract students and companies from all over the world. Another goal of the program is to facilitate knowledge circulation, through the use of HSD Cafés, international and local events and conferences, research and publications, usage of social media. To encourage knowledge sharing, HSD focuses on human capital: businesses with a lot of human resources and the creation of academic programs such as the Cyber Security Academy (run jointly by Leiden University, Delft University of Technology and the Hague University for Applied Sciences), the Security Talent Community (that brings together students and professionals), the Hague Security Academy and the International Cyber Security Summer School. To achieve its goals, HSD implemented a system that enables cooperation between

three sectors to help stimulate the development of security-related innovations, those sectors are: academia, businesses and government agencies.

Some of the HSD programmes are related to: the Internet of Things, big data, financial fraud, satellite technology, quantum computers, digital forensics, sensing, integrated area protection, real-time intelligence, and smart and secure resilient cities.

As part of their 2015-2018 plan, the most urging issues addressed by HSD are centered around five themes:

- Weak signals and the capacity to anticipate events with big data;
- Interconnected security, the Internet of Things and the consequences for critical infrastructures and society;
- Crime and conflict in cyberspace; the impact of cybercrime in daily life and how to fight it;
- Expansion of forensics in the digital world and its linkage with IT to increase its applications;
- Structural use of unmanned systems, their expansion and impact for commercial operations.

The Hague Security Delta forms partnerships and exchanges information with other security clusters in Europe, the USA, Canada, Singapore and South Africa.

In 2016, the HSD had 239 partners, including eleven founding partners such as the City of the Hague, De Haagse Hogeschool, Delflt University of Technology, FoxIT, KPN, Ministry of Economic Affairs, Ministry of Security and Justice, Siemens, Thales, TNO.

- **Agents in charge** :

1) The project was initiated by several research facilities and independent organisations: The Netherland Organisation for applied scientific research (TNO), the consultancy firm Twynstra Gudde, The Hague University of Applied Sciences, The Hague Center for Strategic Studies (HCSS), The Hague Chamber of Commerce, Netherlands Forensic Institute and West Holland Foreign Investment Agency.
2) The HSD Foundation is comprised of the HSD Executive Board, HSD Executive Committee and the HSD Office.

- **Costs** :

The program cost EUR 2,367,000 in 2016:

- EUR 1,019,000 in personnel;
- EUR 1,107,000 for program and projects costs;
- EUR 241,000 in operating expenses (ICT, accommodation, finance and control and advice).

- **Sources of funding** :

In 2016:

- EUR 647,000 are contributions from HSD partners;
- EUR 1,581,000 come from operation and project subsidies;
- EUR 138,000 come from other sources.

- **Penalties** : No
- **Incentives** : Three main incentives:
  - Access to market:
    - More than 400 local and international organisations on site;
    - Host to world-renowned organisations such as the Europol European Cyber Crime Centre (EC3), NATO and Eurojust;
    - Host to security events: Nuclear Security Summit, ASIS, Global Cyber Space Conference, Europol Cybercrime Conference;
    - Providing enterprises services such as giving advice, matchmaking, and support;
    - Global exposure, and strong ties with EU, ASIS, Department of Homeland Security and Maryland (USA), Singapore, Invest Ottawa (Canada), UKTI (UK), SIGNUM (Germany);
    - Strategic location, providing easy access to continental Europe and beyond;
    - Advanced logistics and secure IT infrastructure.
  - Access to resources
    - Capital and funds available;
    - Incubator and start-up facilities. HSD provides services to encourage the development of start-ups in its cluster such as: growth capital, expert monitoring, domain-specific expertise, access to the HSD network and also access to international markets via HSD connections;
    - Access to HSD's Security Talent Community, which includes over 160 studies and courses, 46 education providers, 106 jobs and internships and 245 employers.
  - Fiscal advantages
    - Low statutory corporate income tax rate of 25%;
    - Tax Incentives to promote corporate R&D and subsidies for innovation consortia;
    - Favourable tax treatment for expats;
    - Advanced Tax Rulings and certainty on future taxes;
    - Favourable participation exemption regime;
    - Fiscal unity regime to freely offset profits and losses among group members.
- **Challenges** : No

4. Implementation Information

- January 2010: funding from the Ministry of Economic Affairs, Agriculture and Innovation to start first projects.
- November 2010: initiation of the project.
- March 2012: official launch of the Hague Security Delta, as part of a 2-year project with the support of the Municipality of the Hague and the Dutch Ministry of Economics.
- July 2013: the Hague Security Delta is officially established as a foundation.

- February 2014: official opening of the Hague Security Delta Campus by the Ministry of Security and Justice.
- April 2015: The 'Cyber Security Week' is organized at the new campus, where more than 30 workshops, network events, lectures and demonstrations related to cybersecurity took place. The event hosted over 1700 people from 30 different countries, and also 50 national and international journalists.

5. Evaluation

N/A

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.thehaguesecuritydelta.com/

7. Publications

Hohmann, L. (2016). To What Extent is the Triple-Helix-Model of Etzkowitz & Leydesdorff of Use for the Implementation of Smart Governance? - An Analysis Referring on Implemented Triple Helix Constellations. *Glocality*, 2(1). Retrieved from https://www.glocality.eu/articles/10.5334/glo.7/

8. Media Articles

Olah, N. How the Hague is transforming from a City of Justice to a City of Security. April 26th, 2016. Retrieved from: http://www.citymetric.com/business/how-hague-transforming-city-justice-city-security-2004

van den Ijssel, G. Sixty students from home and abroad try to make the internet safer in The Hague. August 21st, 2017. Retrieved from: https://translate.google.ca/translate?hl=en&sl=nl&u=http://denhaagfm.nl/2017/08/21/zestig-studenten-uit-binnen-en-buitenland-proberen-in-den-haag-het-internet-veiliger-te-maken/&prev=search

9. Documents

HSD. Facts and Figures, for January to December 2016. Available at: https://www.thehaguesecuritydelta.com/about

HSD. (2015). The Value of Cooperation: Innovation in Dutch Security in Perspective. Available at: https://www.thehaguesecuritydelta.com/images/The_Value_of_Cooperation.pdf

10. Related Law / Policies / Etc.

Some similar security clusters :
Israeli Cyber Innovation Arena – CyberSpark, in Israel; SIGNUM, in Berlin Germany; Security Network San Diego, in the US; Aerospace Valley World Competitiveness Cluster, in France.

11. Keywords

Public-Private Partnership, Innovation and Economic Development, Industry Clusters

12. Snapshot

- Targeted population: Dutch and international companies and investors
- Geographical scope: The Netherlands
- Policy type: R&D & Economic Development
- Status : Active

Netherlands – SME Cybersecure, Cybersecurity Business Edition

1. Summary

SME Cybersecure is an awareness campaign program funded by the private and public sector to raise awareness, propose solutions and provide tools for Small and Medium Sized Enterprises in the Netherlands regarding cybercrime. This campaign involves a bus tour in different regions of the country with a promotional team and advisors to meet entrepreneurs and discuss cybersecurity.

2. Nature

Capacity Building; Law Enforcement and Prevention.

3. Policy's Description

- **Date** :
  - August 2015: start date.
  - December 2015: end date.
- **Country** : Netherlands
- **Geographical scope** : Netherlands
- **Instigator** :
  MKB-Nederland (Midden En Klein Bedrijf or SME Netherlands). MKB Nederland is an association of SMEs in the Netherlands, that represents over 170,000 affiliated members.
- **Targeted issue / situation** :
  Small and Medium Sized Enterprises (SMEs) are not always aware of the dangers of cybercrime, and many of them do not have the capacity or the means to take care of the problem. Cyber-attacks account for 8.8 billion euros of loss in the Netherlands, and 75% comes at the expense of entrepreneurs. Therefore, there is a need to raise awareness in the commercial domain in the Netherlands to reduce those costs.
- **Targeted population** : Small and Medium-Sized Enterprises (SMEs)
- **Goals of the policy** :
  - Raise awareness about cybercrime and its impact on businesses to encourage entrepreneurs and SMEs (Small and Medium-Sized Enterprises) to take action to improve their security.
  - A sub-goal is to contribute to the reduction of fear regarding cybercrime, by raising awareness among enterprises.
  - Another sub-objective is to get 300 entrepreneurs to raise their security by giving away free social hacks.

- These social hacks consist in a report of the enterprises' vulnerabilities and the possible countermeasures they can apply

- **Components of the policy** :

Awareness campaigns:

- The "MKB Buzz":
  - A big orange city bus that rides in the different regions of the country.
  - This bus stops in businesses areas or shopping malls and starts the campaign.
  - A promotion team invites entrepreneurs inside the bus: Advisors from KPN (Koninklijke PTT, a mobile telecommunication company) and the Dutch Association of Insurers (an insurance company) are in the bus to greet and inform entrepreneurs about cybercrime and the possible means of prevention.
  - Entrepreneurs are also offered a 'social' hack to give them insight to their vulnerabilities. A maximum of 300 social hacks are provided. These social hacks consist of an immediate report of the results of the hack.
  - With KPN involved, entrepreneurs can access professional services ^{at} a discount. And with the Dutch Association of Insurers, they can get information about cyber-insurance.
- The roadshow also includes:
  - Information program and seminars;
  - Promotion team;
  - Media attention;
  - Digital magazine with interviews with experts and local authorities.

- **Agents in charge** :

MKB-Nederland, the Dutch Network Group (publishing agency for entrepreneurs), the Electronic Commercial Platform, KPN (Dutch Telecom and IT service provider), het Verbond van Verzekeraars (The Dutch Association of Insurers), ThreadStone and the Regional Networks for Safe Entrepreneurship (RPC's) developed the project together.

Different roles for all the organisations within the Cybersecure program:

1) Ministry of Security and Justice: funding of the project;
2) MKB-Nederland: responsible for project management;
3) Dutch Network Group (DNG): project management and data collection;
4) Electronic Commerce Platform: provider of the campaign website and application process for the social hacks;
5) ThreadStone: processing of the social hacks and providing reports to SMEs and their IT teams;
6) Verbond van Verzekeraars: providing cyber insurance options against cybercrime and damages;
7) KPN: provide offers for SME with protection against cybercrime;
8) Regional networks for safe entrepreneurship (RPC's): development of an attractive regional

program for this project to raise awareness regarding cybercrime for SMEs.

- **Costs** :

  EUR 491,900 total:

  - EUR 72,400 for project preparation (infrastructure, communication, service and support);
  - EUR 83,900 by region (5 regions) for the roadshows, recruitment, organization, social hacks (14,000), support, data collection and IT.

- **Sources of funding** :

  - Dutch Ministry of Security and Justice granted EUR 476,900.
  - Verbond of Verzekeraars allocated EUR 15,000.

- **Penalties** : No

- **Incentives** : SMEs are offered a free hack to assess their cybersecurity level.

- **Challenges** : No

4. Implementation Information

- August 2015: start date.
- October 2015: roadshow start date.
- December 2015: end date. End of roadshow and expected evaluation.

5. Evaluation

- **Existence of an evaluation** : Yes, 2 evaluations.

- **Evaluation type** : Internal evaluation of the process.

- **Evaluator** :

  1. MKB-Nederland and the Ministry of Security and Justice.
  2. MKB-Nederland.

- **Methodology** :

  1. The first evaluation presents the results up to October 2015.
  2. The second evaluation presents the final results, in December 2015.

- **Outcomes** :

  1. Online results:
     - 235 entrepreneurs have subscribed for the social hack;
     - 149 social hacks carried out.
  2. Offline results:
     - 4 of 7 roadshows have taken place;
     - 3 of 5 regions were visited;

- 750 entrepreneurs have been reached by the promotion team.

3. Conclusion:
- Positive feedback from SMEs about the campaign and the hacks;
- Still a lack of awareness, based on the 50% of no show after feedback appointment (from hacks).

4. Evaluation:
- 58% SMEs state having raised their awareness following the campaign;
- 45% took measures after enrollment into the program (1 in 5 made improvements regarding Wifi and IT protocols);
- 25% did it after the hack;
- 83% of the hacked SMEs put cybercrime on their agenda;
- 77% did not consider taking insurance;
- Before the hack, 72% didn't put their network on regular check, but after the hack 84% considered doing regular checkups;
- Not all 300 hacks were sold;
- SMEs didn't give enough priority to the feedback of their hack;
- 75% of hacked SMEs are insufficiently protected.

6. URL

http://magazine.veiligzakelijkinternetten.nl/aa#
https://www.veiligzakelijkinternetten.nl/

7. Publications

MKB-Nederland. (2015). European Crime Prevention Award (ECPA) Entry – Netherlands. Retrieved from http://eucpn.org/document/sme-cybersecure-cybersecurity-business-edition

Jacobs, E. (December, 2015). *To make entrepreneurs aware of cybercrime*. Presented at the ECPA, in Luxembourg. Presentation retrieved from http://eucpn.org/document/sme-cybersecure-cybersecurity-business-edition

Europol's European cybercrime Center. (2016). *The EC3 Bulletin*. Issue 7, 1-19.

8. Media Articles

SGMAI Secretaria Geral. Netherlands Win the European Crime Prevention Award 2015. December 22nd, 2015. Retrieved from https://translate.google.ca/translate?hl=en&sl=pt&u=http://www.sg.mai.gov.pt/Noticias/Paginas/ECPA-2015.aspx&prev=search

9. Documents

N/A

10. Related Law / Policies / Etc.

N/A

11. Keywords

SMEs, Cybercrime Prevention, Awareness

12. Snapshot

- Targeted population: SMEs
- Geographical scope: Netherlands
- Policy type: Capacity Building, Law Enforcement and Prevention
- Status: Inactive

United Kingdom

1) Cyber Essentials
2) Cyber Schools Programme
3) Cybersecurity Challenge

UK – Cyber Essentials

1. Summary

Cyber Essentials is a cyber security standards scheme backed by the British government that applies to organisations and businesses in the UK. Organisations must make an assessment of their level of security or ask a third party to produce that assessment to obtain a Cyber Essentials badge. This badge attests that they satisfy the government's cyber security standards. This scheme aims to encourage businesses to protect their systems and their customers' sensible information.

2. Nature

Capacity Building; Standardization and Accreditation; Economic Incentives and Nudging

3. Policy's Description

- **Date** :
  - June 2014: Implementation.
- **Country** : United Kingdom.
- **Geographical scope** : United Kingdom.
- **Instigator** : The Department for Business, Innovation and Skills
- **Targeted issue / situation** :
  Risk management practices to address basic cyber security threats and restoring trust between customers and the businesses that possess their confidential information.
- **Targeted population** :
  Businesses and organisations in the UK, especially Small and Medium-sized Enterprises (SMEs).
- **Goals of the policy** :
  Two main goals:
  - Implement cyber security standards for all organisations to mitigate the risks from basic internet threats;
  - Reassure customers, investors, insurer and others that cyber security measures are taken by these organisations.

  Focuses on 5 key aspects of cyber security:
  - Secure configuration;
  - Boundary firewalls and internet gateways;
  - Access control and administrative privilege management;
  - Patch management;

- Malware protection.

- **Components of the policy** :

There are two sets of cyber essentials standards:

- Cyber Essentials, where organisations must complete a self-assessment questionnaire that will later be reviewed by an external certifying body;
- Cyber Essentials Plus, where tests of the organisation's systems are done by the external Certifying body.

Both standards include a questionnaire that assesses security controls and secure configurations of the organisation's computing resources (CREST).

Once an organisation responds to the Cyber Essentials criteria, it receives a badge that certifies their level of cybersecurity and that they can use it in their promotional material.

The Cyber Essentials documents are free. The costs of the annual certification for Cyber Essentials are about GBP 300 for networks with up to 250 employees and 16 IP address ranges. Cyber Essentials Plus can cost from GBP 1000–2000, and more, depending on the size and complexity of the network. Also, to get Cyber Essentials plus, an organization must get the basic accreditation and the costs are cumulative.

- **Agents in charge** :

1) The Department of Business Innovations and Skills launched the scheme;
2) The Communications-Electronics Security Group (CESG), which is the information security branch of GCHQ, required CREST (a non-profit organisation that does ethical security testing) to develop the assessment framework for the Scheme.
3) The Information Assurance for Small & Medium Enterprises (IASME), the Information Security Forum (ISF), and the British Standards Institution (BSI) as well as other professional bodies and individual businesses, backed by the government, have also worked in a collaborative effort to develop the Scheme.
4) Once the Scheme was implemented: the certifying bodies are: CREST, CESG, IASME, APMG Group and OG Business Group.

- **Costs** : N/A
- **Sources of funding** : Government funding
- **Penalties** : N/A
- **Incentives** :

Holding a Cyber Essentials badge is mandatory to bid for governmental contracts. Also, having a badge should encourage customers to conduct business with organisations that are certified by Cyber Essentials.

- **Challenges** : No

4. Implementation Information

- 2012: the British Government launched the 10 Steps to Cyber Security Guide.
- November 2013: an evaluation of the program concluded that there were no standards of cyber security that met the requirements of the government.
- June 2014: Cyber Essentials was implemented.
- October 2014: all government suppliers bidding for government contracts must have a Cyber Essentials badge.

5. Evaluation

- **Existence of an evaluation** : Yes
- **Evaluation Type** : Empirical, made by a research agency.
- **Evaluator** :

  The DCMS (Department for Digital, Culture, Media & Sport) commissioned Kantar Public (formerly known as the TNS BMRB) to conduct an evaluation of Cyber Essentials.
- **Methodology** :

  Qualitative research on 63 businesses. There are 3 steps to this research:
  - A process evaluation, done with 30 in-depths interviews with businesses that are certified by Cyber Essentials;
  - A message testing evaluation, done with 4 focus group that included non-certified businesses;
  - A remote web testing, performed with 11 SMEs that are not certified, to evaluate their responses to the information provided by the Cyber Essentials' website.
- **Outcomes** :

  Key findings:
  - "Motivations amongst early adopters of the scheme have been to (a) satisfy mandatory government procurement requirements or (b) enable them to sell the scheme to other businesses, leading to a relatively high concentration of expert cyber and IT consultants in the audience" (TNS BMRB, 2016);
  - Security was rarely the main reason for businesses to get certified. But the businesses that were mainly concerned by cyber security, were most likely victims of previous breaches and threats;
  - Low awareness of the scheme outside of the cyber and IT sectors is also a clear barrier (in 2016, only 6% of businesses knew about Cyber Essentials);
  - In general, businesses found that the certification process was simple and efficient. Although, lack of clarity about the costs, process and requirements and the technical jargon were sometimes confusing;
  - There were too many Certifying Bodies (CBs) that used different approaches for the

certification, which made it more difficult for the businesses to choose the appropriate CBs. It also caused a lack of standardisation:

- Most certified businesses heard about Cyber Essentials because it was mandatory to bid for government contracts;
- IT and security related companies were more likely to have heard of the scheme.

6. URL

https://www.cyberaware.gov.uk/cyberessentials/

7. Publications

CREST (2017). Cyber Essentials – Keeping UK Businesses Safe. Available at: http://www.cyberessentials.org/

IT Governance (2017). Cyber Essentials – What is Cyber Essentials? Available at: https://www.itgovernance.co.uk/cyber-essentials-scheme

IASME Consortium (2017). Cyber Essentials Scheme. Available at: https://www.iasme.co.uk/cyberessentials/

BSI Group (2017). Cyber Essentials Scheme. Available at: https://www.bsigroup.com/en-GB/Cyber-Security/cyber-essentials/

TNS BMRB. (2016). Cyber Essentials Scheme – process evaluation and communications testing. Available at: https://www.gov.uk/government/publications/cyber-essentials-scheme-research

8. Media Articles

GOV.UK. Cyber Essentials Scheme: overview. April 7th, 2014. Retrieved from: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

NCSC. Scheme – Cyber Essentials. November 25th, 2015. Retrieved from: https://www.ncsc.gov.uk/scheme/cyber-essentials

Dunn, J. E. Cyber Essentials – what UK SMEs need to know about the Government's cybersecurity scheme. November 6th, 2015. Retrieved from: http://www.techworld.com/security/cyber-essentials-what-uk-smes-need-know-about-government-scheme-3629001/

Computer Weekly. Cyber Risk and the UK's Cyber Essentials Scheme. June 2015. Retrieved from: http://www.computerweekly.com/opinion/Cyber-risk-and-the-UKs-Cyber-Essentials-Scheme

Morbin, T. Cyber Essentials: benchmarking best practice. September 1st, 2014. Retrieved from: https://www.scmagazineuk.com/cyber-essentials-benchmarking-best-practice/article/541530/

9. Documents

N/A

10. Related Law / Policies / Etc.

UK's National Cyber Security Programme.

11. Keywords

Standards, Risk Management, Cybercrime Prevention, SMEs

12. Snapshot

- Targeted population: SMEs and businesses
- Geographical scope: United Kingdom
- Policy type: Capacity Building; Standardization and Accreditation; Economic Incentives and Nudging
- Status: Active

UK – Cyber Schools Programme

1. Summary

The Cyber Schools Programme aims to encourage students between the ages of 14 and 18 to develop essential skills in cyber security and help defend the nation's economy and businesses against online breaches and threats. The pilot project for this extracurricular programme will be launched in September 2017. Its main goal is to reduce the expected skills shortage in cyber security.

2. Nature

Workforce Development

3. Policy's Description

- **Date** :
  - February 2017: announcement and notice of tenders to set up the Cyber Schools Programme.
  - September 2017: Pilot launch expected in England only.
  - 2021: The program aims to train a minimum of 5700 teenagers by 2021.
- **Country** : United Kingdom
- **Geographical scope** : United Kingdom
- **Instigator** :
  Department for Culture, Media and Sport (DCMS), as part of the Government's National Cyber Security Programme, and under the Cyber First brand.
- **Targeted issue / situation** :
  Experts are predicting a shortage of cybersecurity experts in the coming years. Britain seeks to develop a skilled workforce that will support strong cyber defence capacities.
- **Targeted population** :
  Motivated and talented British teenagers, aged between 14 and 18 years old.
- **Goals of the policy** :
  Primary goal: To defend Britain against the rising threats of online attacks.
  Secondary goals:
  - To teach teenagers the required skills to grow in the cybersecurity sector;
  - To guard against a future cyber skills shortage.

The program aims to give young people an opportunity to develop the skills and knowledge on subjects critical to cybersecurity, like maths, engineering, computing, finance and behavioural psychology, but also help them understand the major impact of cybersecurity on the economy.

- **Components of the policy** :
  - To get onto the programme, students will need to go through a selection testing to ensure they have a certain level of enthusiasm and motivation, as well as a high cyber aptitude, either latent or developed.
  - Older teenagers can also join at any point, if they can meet the requirement for the programme and pass a selection testing.
  - This extra curriculum will “mix classroom and online teaching with real-world challenges and hands-on work experience” (Sky News, 2017).
  - Experts from the cybersecurity industry will be mobilised to inspire, teach and expose the children to possible future career options.
  - Students will have to commit four hours a week, starting at the age of 14 for four years. These hours will be flexible around exams and busier study periods.
- **Agents in charge** :
  The DCMS is evaluating tenders and recruiting service providers to develop the extracurricular program.
- **Costs** : GBP 20 million committed until 2021.
- **Sources of funding** : The DCMS funds the programme.
- **Penalties** : N/A
- **Incentives** : No
- **Challenges** : No

4. Implementation Information

- The pilot is expected to launch in September 2017 in England.
- The program will be evaluated and reviewed after the first year.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.gov.uk/guidance/cyber-schools-programme

7. Publications

Government of UK. Cyber Schools Programme. February 17th, 2017. Retrieved from: https://www.gov.uk/guidance/cyber-schools-programme

Government of UK. Extracurricular cyber clubs to inspire and identify tomorrow's cyber security professionals. February 11th, 2017. Retrieved from: https://www.gov.uk/government/news/extracurricular-cyber-clubs-to-inspire-and-identify-tomorrows-cyber-security-professionals

National Cyber Security Centre. Fresh drive to develop next generation of cyber security experts. February 3rd, 2017. Retrieved from: https://www.ncsc.gov.uk/news/fresh-drive-develop-next-generation-cyber-security-experts

8. Media Articles

Dearden, L. British teenagers to be taught 'cyber curriculum' to defend UK against threat of hacking attacks. February 11th, 2017. Retrieved from: http://www.independent.co.uk/news/uk/home-news/cyber-attacks-security-uk-russia-china-isis-terrorist-nhs-websites-curriculum-school-teenagers-a7574611.html

Rajab, T. DCMS announces new Cyber Schools Programme. February 13th, 2017. Retrieved from: https://www.techuk.org/insights/news/item/10237-dcms-announces-new-cyber-schools-programme

Williams, H. UK government to deliver 'cyber curriculum' to tackle cyber security shortage. February 13th, 2017. Retrieved from: http://www.cbronline.com/news/cybersecurity/uk-government-cyber-curriculum-tackle-cyber-security-skills-gap/

Computer Business Review. UK government pledges £1.9bn investment as two-thirds of big UK businesses hit by cyber security breaches. May 9th, 2016. Retrieved from: http://www.cbronline.com/news/mobility/security/uk-government-pledges-19bn-investment-as-two-thirds-of-big-uk-businesses-hit-by-cyber-security-breaches-4886973/

Delta eSourcing. Department for Culture, Media and Sport: Cyber Schools Programme - Notice summary. February 2nd, 2017. Retrieved from: https://www.delta-esourcing.com/tenders/UK-title/5DGJ787HC7

Raywood, D. Help save the youth. February 13th, 2017. Retrieved from: https://www.infosecurity-magazine.com/news-features/help-save-the-youth-of-cyber/

Jardine, K. Cyber Resilience: Cyber news and threats. February 20th, 2017. Retrieved from: https://blogs.gov.scot/cyber-resilience/2017/02/20/cyber-news-and-threats-20th-feb/

Sky News. 'Cyber curriculum' to defend UK against attacks. February 11th, 2017. Retrieved from: http://news.sky.com/story/cyber-curriculum-to-defend-uk-against-attacks-10763378

9. Documents

N/A

10. Related Law / Policies / Etc.

The programme will complement a number of government initiatives such as the 'Cyber Retraining Academy' and the 'Cyber Security Apprenticeships for Critical Sectors Scheme'.

The programme is part of the Government's 'National Cyber Security Programme', that also announced the 'Cyber First' bursary funding scheme that offer grants to 1000 students in a relevant degree.

11. Keywords

School Training, Extracurricular Activities

12. Snapshot

- Targeted population: Teenagers, 14-18 year olds
- Geographical scope: United Kingdom
- Policy type: Workforce Development
- Status: Active

UK – Cybersecurity Challenge

1. Summary

Cyber Security Challenge UK is a non-profit organization supported by the British government, academia and industry that runs a series of national competitions, learning programmes, and networking initiatives. It is designed to identify, inspire and encourage people to become cybersecurity professionals and be part of the industry. The Challenge was inspired by a similar initiative in the United States, and aims to reduce the expected shortage of qualified individuals in cyber security.

2. Nature

Workforce development

3. Policy's Description

- **Date** :
  - March 2010: Launch of the initiative.
  - July 2010: First challenge organized.
- **Country** : United Kingdom
- **Geographical scope** : United Kingdom
- **Instigator** :
  Cyber Security Challenge UK with the help of the SANS Institute (SysAdmin, Audit, Network and Security Institute) and other businesses, academia, and government agencies including QinetiQ, Royal Holloway University, the Cabinet Office and professional bodies like IISP (Institute of Information Security Professionals).
- **Targeted issue / situation** :
  There is a skill shortage and a growing demand in the cybersecurity field. Britain seeks to build a specialized and professional workforce.
- **Targeted population** :
  - Preference for students and teenagers in the UK.
  - All British or European citizens living in the UK over 16 years old are eligible.
  - If the participant currently works in the Cybersecurity profession, he/she cannot attend a face-to-face competition or win a career enabling prize.
  - Each type of competition targets different groups of youths in the UK.
- **Goals of the policy** :
  The objective is to encourage talented individuals in taking up careers in the cybersecurity field.

- **Components of the policy** :

The main Challenge: the first round of the competitions occurs online, followed by a face-to-face round, with winners going through to a final masterclass challenge:

1. Online qualifiers with the 'Play On Demand' (POD) platform, where contestants can play directly online and 'CyPhinx', a 3D immersive downloadable platform with games similar to POD, but with a faster pace and a more interactive environment;
2. Face-to-face competition, during weekends all-through the year;
3. Masterclass Final: 42 of the best from the participants of the face-to-face competitions are invited at the end of the year to the Masterclass. All Masterclass participants receive prizes from the sponsors, but there is only one final winner. "Prizes are all career-enabling opportunities such as specialised training, internships and memberships of security organisations that will be tailored to the winning individuals and teams" (Baker, 2010, in Ashford 2010).

Some additional competitions run by the Cyber Challenge are:

- Cyber Games (12-16 years old);
- Cyber Centurion (teams of four, 12 to 18 years old);
- Extended Project qualification (to help apply to university);
- Capture the Flag (CTF) competition.

- **Agents in charge** :

The program is run by a management consortium of cybersecurity professionals across the public and private sectors and academia. Every year, a different group or agency is in charge of preparing the annual Challenge:

1) 2010: QinetiQ and SANS Institute;
2) 2012: Sophos;
3) 2013: HP, Cassidian CyberSecurity UK;
4) 2014: British Telecom, GCHQ, the National Crime Agency, Juniper Networks, Lockheed Martin;
5) 2015: British Telecom, GCHQ, the National Crime Agency, Lockheed Martin, Juniper Networks and Airbus Group;
6) 2016: Protection Group International (PGI) for the face-to-face, and PWC for the Masterclass;
7) 2017: PGI for the face-to-face, and British Telecom for the Masterclass.

- **Costs** : Unknown

- **Sources of funding** :

There are a total of 75 sponsors to the Cyber Security Challenge. The contributions can be financial or a combination of financial and value in kind. There are more than 75 sponsors at various levels of commitment.

- **Penalties** : No

- **Incentives** : N/A
- **Challenges** : No

4. Implementation Information

Launched in March 2010 and implemented in July 2010 with the very first Challenge.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://cybersecuritychallenge.org.uk/

7. Publications

Cheung, R. S., Cohen, J. P., Lo, H. Z., & F. Elia. (2011). Challenge Based Learning in Cybersecurity Education. In *Proceedings of the 2011 International Conference on Security & Management (1)*. Available at: http://www.lidi.info.unlp.edu.ar/WorldComp2011-Mirror/SAM5063.pdf

Cyber Security Challenge UK (2017). Inside CYBER: Bringing you the inside track on cyber security – Pilot. *Inside Cyber, 1*, pp.1-19. Available at: https://www.cybersecuritychallenge.org.uk/app/uploads/2017/02/Inside-Cyber-01-MCN1265.pdf

Cyber Security Challenge UK (2017). Inside CYBER: Bringing you the inside track on cyber security. *Inside Cyber, 2*, pp.1-45. Available at: https://www.cybersecuritychallenge.org.uk/app/uploads/2017/03/Edition-1-Inside-Cyber-March-2017.compressed.pdf

Demchak et al. (2016). United Kingdom Cyber Readiness at a Glance. *Potomac Institute for Policy Studies*, pp. 1-32. Retrieved from http://www.potomacinstitute.org/images/CRI/FINALCRIUSProfile13Oct.pdf

Downing, E. (2011). Cyber security-A new national programme. *Science and Environment Section*, *House of Commons*, 3-9. Available at: https://www.scribd.com/document/133611400/Downing-Cyber-Security-pdf

8. Media Articles

Computer Weekly. NCA competition launches 2015 Cyber Security Challenge UK. May 16th, 2014. Retrieved from: http://www.computerweekly.com/news/2240220800/NCA-competition-launches-2015-Cyber-Security-Challenge-UK

Gatekeeper.UK cyber security challenge launches to find the next generation of security experts. April 28th, 2010. Retrieved from: http://www.secureforce.com/blog/item/8-uk-cyber-security-challenge-launches-to-find-the-next-generation-of-security-experts

Ashford, W. UK launches Cyber Security Challenge. July 25th, 2010. Retrieved from: http://www.computerweekly.com/news/1280093346/UK-launches-Cyber-Security-Challenge

Leyden, J. Opening UK cyber-security challenge cracked. July 27th, 2010. Retrieved from: http://www.theregister.co.uk/2010/07/27/uk_challenge_cipher_cracked/

Baker, J. The Cyber Security Challenge UK – Getting the right cyber security talent in place. October 2nd, 2012. Retrieved from: http://www.thesecurityco.com/news/the-insider/archive-2012/october-2012/the-cyber-security-challenge-uk/

McCaskill, S. Cyber Security Challenge UK Announces First Finalists. January 16th, 2012. Retrieved from: http://www.silicon.co.uk/workspace/cyber-security-challenge-uk-announces-first-finalists-54451?inf_by=594d7464671db8e86d8b49ad

Leyden, J. Soon-to-be Facebook intern wins UK Cyber Security Challenge. March 17th, 2017. Retrieved from: https://www.theregister.co.uk/2014/03/17/cyber_security_challenge_final_winner_cambridge_student/

GOV. GCHQ supports Cyber Security Challenge UK's 2015 Masterclass. November 13th, 2014. Retrieved from: https://www.gchq.gov.uk/news-article/gchq-supports-cyber-security-challenge-uks-2015-masterclass

Maltego Magician (2013, March 11) Cyber Security Challenge – The Masterclass. March 11th, 2013. Retrieved from: https://itgeekchronicles.co.uk/2013/03/11/cyber-security-challenge-the-masterclass/

9. Documents

N/A

10. Related Law / Policies / Etc.

Inspired by US Department for Defense Cyber Crime Center (DC3) Digital Forensics Challenge

US CyberPatriot Competition

SANS Cyber Academy

GCHQ's Cyber First

European Cyber Security Challenge

11. Keywords

Cybersecurity Competition, Workforce Development

12. Snapshot

- Targeted population: Youths and students
- Geographical scope: United Kingdom
- Policy type: Workforce development
- Status: Active

United States of America

1) Centers of Academic Excellence in Cyber Defense (CAE-CD)
2) Cybersecurity Information Sharing Act of 2015 (CISA)
3) National Institute of Standards and Technology (NIST) Cybersecurity Framework
4) National Institute of Standards and Technology CyberSeek (NIST CYBERSEEK)

USA – Centers of Academic Excellence in Cyber Defense (CAE-CD)

1. Summary

American Federal government program aiming to promote education in cyber defense, produce professionals with cybersecurity expertise and strengthen national information infrastructure. Led by the National Security Agency (NSA) and the Department of Homeland Security (DHS), this program designates select academic and vocational institutions of Centers of Academic Excellence in Cyber Defence. Institutions interested in receiving the designation must complete a rigorous application process which involves mapping its computer science curriculum to strict standards established by the federal government. The program and its curriculum mapping process have been heavily referenced and reviewed by different members of the computer science community, but its benefits remain unclear.

2. Nature

Workforce Development

3. Policy's Description

- **Date** :
  - 1998: Creation of the National Centers of Academic Excellence in Information Assurance Education (CAE-IAE) by the NSA.
  - 2004: DHS joins as a partner.
  - 2008: CAE in Information Assurance Research (CAE-I-R) component added to program.
  - 2010: Two-Year Education (CAE-2Y) component added.
- **Country** : United States of America
- **Geographical scope** : United States of America
- **Instigator** :

  U.S. Government (Clinton Administration).

  A Presidential Decision Directive (PDD-63) by the Clinton government on Critical Infrastructure Protection from May 22nd 1998 states that: "[conferences will be considered] that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field".
- **Targeted issue / situation** :

  Increasing the number of qualified cybersecurity professionals needed to protect government and industry networks.

- **Targeted population** :
  - Academic and Educational institutions who wish to be recognized for offering a designated cybersecurity education. Educators/Professors/Instructors who are interested in teaching cybersecurity classes.
  - Students looking to work in the cybersecurity field.
  - Employers looking to hire graduates with specific cybersecurity skills.
- **Goals of the policy** :
  - The primary goal of the program is to reduce vulnerability in American information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise.
  - The secondary goal of the program is to create and maintain high quality cybersecurity-related degree programs that meet strict cybersecurity academic standards and to create a common body of knowledge, information and best practices for American information security.
  - These goals are achieved by designating select institutions as Centers of Academic Excellence. This designation aims to attract students to institutions which have mapped their computer science (CS) curriculum to strict government standards in cyber defense and in turn generate out more graduates specialized in this field.
- **Components of the policy** :
  - Academic Institutions interested in receiving CAE-CD designation must complete an application. Institutions can apply as a CAE in Four-year+ Education (CAE-CDE), Two-year Education (CAE-2Y), or Research Designation (CAE-R). They may also apply to a CAE-CD Focus Area (FA).
  - The CAE-CDE is the base designation for all undergraduate and some graduate-level cyber defense programs. The CAE2Y component gives technical colleges, government training centers and other two-year institutions the opportunity to receive a CAE designation as well. The research component (CAE-R) encourages advanced and specialized graduate-level cybersecurity research. The Focus Area (FA) allows institutions to be designated as specialized in certain cyber defense areas.
  - To apply, institutions must meet the rigorous levels of academic excellence established by the NSA, based on training standards created by the Committee on National Security Systems (CNSS). These include the CNSS Information Assurance Courseware Evaluation (IACE) standards. This ensures compliance with national standards in cyber defense. Applying institutions must map out their curricula to at least two national training standards.
  - There are knowledge unit matrices and reviewer checklists available to help applying institutions map out what they will offer in terms of topics covered, class objectives, projects, labs and exams. Mapping a course out to these standards may require instructors to reexamine how they would normally teach their class. They may have to adjust course material, assignments, labs and exams to suit the federally appointed curriculum. There are instructional videos,

modules and exercises that faculty can follow to better understand the CNSS standards.

- Once an institution's application to be designated CAE-CD is accepted, there is an official designation ceremony.
- Students who wish to receive an education at a CAE-CD designated institutions must explicitly seek out schools with the designation. CAE-CDs are usually housed in Technology or Computer Science departments. In enrolling in a program of a CAE-CD university department, it is expected that students will be better prepared for federal work in cyber defense. Upon graduation, students receive explicit recognition of having graduated from a CAE-CD.

- **Agents in charge** :

1) The Department of Homeland Security (DHS) and the National Security Agency (NSA) both sponsor the National Centers of Academic Excellence (CAE) program. The NSA is responsible for national Signals Intelligence (SIGINT) and Information Assurance (IA) as well as the protection of American information systems and computer networks. The DHS is responsible for ensuring the safety and protection of the USA at many different levels. These two federal agencies work together to strengthen American information security and systems through the CAE-CD program.
2) In regard to the CAE-CDs, the NSA was responsible for overseeing the criteria for CAE designation, created by the CNSS. It also receives all CAE-CD submission letters and all other communications.
3) It is currently unclear how the DHS contributes to the CAE-CD program beyond being a federal sponsor.

- **Costs** : Unknown
- **Sources of funding** : The program is jointly sponsored by the NSA and the DHS.
- **Penalties** : No
- **Incentives** :

CAE-CD designation comes with formal recognition from the American government, which carries some prestige. However, CAE designation does not carry a commitment of funding from the NSA or DHS. Funding opportunities are periodically available exclusively to CAE-CD institutions; however, they are not guaranteed and funding details are unknown. Students enrolled at CAE-CD institutions may apply for the Federal Cyber Service Scholarship for Service Program as well as for the Department of Defense Information Assurance Scholarship Program.

- **Challenges** : N/A

4. Implementation Information

- 1998: PDD-63 establishes that education in information security is a priority to the American

nation. The original National CAE in Information Assurance Education (CAE-IAE) program is created by the NSA.

- 2004: The DHS joins as partner to the CAE-IAE program.
- 2008: CAE in Information Assurance Research (CAE-I-R) component added to program to encourage graduate-level research in cybersecurity.
- 2010: Two-Year Education (CAE-2Y) component added to allow two-year institutions, technical schools, and government training centers the opportunity the receive a CAE designation.

The term “Information Assurance Education” was replaced by “Cyber Defense” at an unspecified date.

The program was supplemented by scholarships programs funded by the U.S. National Science Foundation (NSF) and the U.S. Department of Defense (DoD) at an unspecified date.

Finally, according to an undated handout available on the National Initiative for Cybersecurity Careers and Studies’ (NICCS) website, there are plans to further map the knowledge units established by the NSA and the DHS for the CAE’s with the National Initiative for Cybersecurity Education’s (NICE) Workforce Framework 2.0.

5. Evaluation

- **Existence of an evaluation** : Yes
- **Evaluation type** :

1) Critical analysis and literature review:
   Bishop, M., & Taylor, C. (2009). A Critical Analysis of the Centers of Academic Excellence Program. In *Proceedings of the 13th Colloquium for Information Systems Security Education*, Seattle, WA, 1–3. Retrieved from http://nob.cs.ucdavis.edu/bishop/papers/2009-cisse/caecrit.pdf
2) Empirical quantitative study:
   Cooper, S., Nickell, C., Pérez, L. C., Oldfield, B., Brynielsson, J., Gökce, A. G., Hawthorne, E. K., Klee, K. J., Lawrence, A. & Wetzel, S. (2010). Towards Information Assurance (IA) Curricular Guidelines. In *Proceedings of the 2010 ITiCSE Working Group Reports,* New York, NY, 49–64. Available at ACM: https://doi.org/10.1145/1971681.1971686
3) Empirical mixed methodology studies:
   Kallberg, J., & Thuraisingham, B. (2012). Towards cyber operations – The new role of academic cyber security research and education. In *2012 IEEE International Conference on Intelligence and Security Informatics*, 132–134). Available at IEEE Xplore: https://doi.org/10.1109/ISI.2012.6284146

Taylor, C., Alves-Foss, J., & Freeman, V. (2006). An academic perspective on the CNSS standards: a survey. In *Proceedings of the 10th Colloquium for Information Systems Security Education*, 39–46. Available from CISSE: https://cisse.info/resources/archives/category/6-papers

- **Evaluator** : Mostly independent academic researchers.
- **Methodology** :

  Taylor, Alves-Foss & Freeman (2006) analysed quantitative and qualitative survey responses from 56 CAE and non-CAE institutions teaching IA (112 institutions were surveyed) that had met CNSS IACE requirements. The survey assessed participants' experiences with mapping their curriculum to the CNSS standard. Later, Bishop & Taylor (2009) conducted a critical, argumentative literature review of the existing knowledge on the process to apply as a CAEAIE designated institution. Cooper et al. (2010) then looked at 29 quantitative surveys from 117 CAEs asking for institutional information and curricular content according to a list of various computer science topics. Each institution was then asked what percentage they felt covered each topic and what percentage it should cover. Finally, Kalberg & Thuraisingham (2012) looked at how CAE-R institutions differ from traditional IAE institutions by looking at all 48 CAE-R websites and evaluating them against a list of criteria the researchers deemed to be important in cyber-operations research.

- **Outcomes** :

  Taylor et al. (2006) found that, although the CNSS mapping process is an effective marketing tool, it is outdated and does not give good guidance for computer science curriculum mapping to academic requirements. Furthermore, Bishop and Taylor (2009) also argued that the process to apply for CAEAIE designation is time consuming and challenging. They mention that the lack of resources allocated to CAEIAEs as a barrier proper IAE as well. Cooper et al. (2010), found that participants desired change in how many course topics were covered, for example, by spending more time on digital forensics and less time on network security. Finally, Kalberg & Thuraisingham (2012) noticed that the minority of CAE-R institutions adopt a multidisciplinary approach and venture into different branches of cyber operations research, such as cyberspace issues or profoundly look at privacy concerns from a legal standpoint.

6. URL

https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

7. Review

Bacon, T., & Tikekar, R. (2003). Experiences with Developing a Computer Security Information Assurance Curriculum. *Journal of Computing Sciences in Colleges, 18*(4), 254–267. Available at ACM: http://dl.acm.org/citation.cfm?id=767598.767640

Bogolea, B., & Wijekumar, K. (2004). Information Security Curriculum Creation: A Case Study. In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development,* New York, NY, 59–65. Available at ACM: https://doi.org/10.1145/1059524.1059537

Conklin, A. (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences.* Available at IEEE Xplore: https://doi.org/10.1109/HICSS.2006.110

Conti, G., Hill, J., Lathrop, S., Alford, K., & Ragsdale, D. (2003). A Comprehensive Undergraduate Information Assurance Program. In C. Irvine & H. Armstrong (Eds.), *Security Education and Critical Infrastructures*, 243–260. Available at Springer: https://doi.org/10.1007/978-0-387-35694-5_23

Crowley, E. (2003). Information System Security Curricula Development. In *Proceedings of the 4th Conference on Information Technology Curriculum,* New York, NY, 249–255. Available at ACM: https://doi.org/10.1145/947121.947178

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. *Journal of Information Systems Education*, *13*(3), 177-182. Retrieved from http://jise.org/Volume13/Pdf/177.pdf

Schweitzer, D., Humphries, J., & Baird, L. (2006). Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education. *Journal of Computing Sciences in Colleges*, *22*(1), 151–160. Available at ACM: http://dl.acm.org/citation.cfm?id=1181833

Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security*, *26*(4), 290–299. Available at ScienceDirect: https://doi.org/10.1016/j.cose.2006.11.005

Spafford, E. H. (2009). Cyber Security: Assessing Our Vulnerabilities and Developing an Effective Defense. In *Protecting Persons While Protecting the People*, Berlin, 20–33. Available at Springer: https://doi.org/10.1007/978-3-642-10233-2_3

Taylor, C., & Alves-Foss, J. (2005). The Need for Information Assurance Curriculum Standards. In *Proceedings of the 9th Colloquium for Information Systems Security Education Georgia Institute of Technology,* 67–74. Retrieved from_ https://cisse.info/resources/archives/category/4-papers?download=31:s04p02-2005

Wilson, A., & Ali, A. (2011). The biggest threat to the U.S. digital infrastructure: The cyber security workforce supply chain. *Academy for Studies in Business Proceedings*, *3*(2), 1. Retrieved from: http://www.alliedacademies.biz/Public/Proceedings/Proceedings29/ASB%20Proceedings%20Fall%202011.pdf

Yurcik, W., & Doss, D. (2000). Information security educational initiatives to protect e-commerce and critical national infrastructures. In *Information systems education conference (ISECON)*. Available at Research Gate: https://www.researchgate.net/profile/William_Yurcik/publication/237430946_Information_Security_Educational_Initiatives_to_Protect_E-Commerce_and_Critical_National_Infrastructures/links/00b7d5

3b163cec6040000000.pdf

8. Media Articles

N/A

9. Documents

CNSS Training Standard No. 4011
http://niatec.info/GetFile.aspx?pid=6

Resources for faculty mapping to CNSS standards
http://niatec.info/ViewPage.aspx?id=105

PDD 63
https://fas.org/irp/offdocs/pdd/pdd-63.htm

10. Related Law / Policies / Etc.

N/A

11. Keywords

Academic Qualifications, Curriculum Design, Accreditation

12. Snapshot

- Targeted population: Academic and Educational Institutions, Educators/Professors/Instructors, Students and Employers
- Geographical scope: USA
- Policy type: Workforce Development
- Status: Active

USA – Cybersecurity Information Sharing Act of 2015 (CISA)

1. Summary

The Cybersecurity Information Sharing Act of 2015 (CISA) is a bill passed in October 2015 that facilitates cybersecurity information sharing between private and public entities in the United States of America. CISA provides protection from different legislation that prohibits the transfer of information between entities in the USA. If shared information can be defined as a "cyber threat indicator" or "defensive measure" per CISA, is stripped of personal data, is transmitted through the appropriate channels, and is shared with the intention of reducing cybercrime, then the sharing entity is granted protection.

2. Nature

Information Sharing

3. Policy's Description

- **Date** : December 2015: Bill passed.
- **Country** : United States of America
- **Geographical scope** : United States of America
- **Instigator** :
  Co-sponsored by Republican Senator Richard Burr of North Carolina and Democratic Senator Diane Feinstein of California.
- **Targeted issue / situation** :
  There is an increase in the number of cyber-attacks on American organizations and companies where the private information of consumers is compromised, resulting in identity theft, fraud and other cyber threats. American corporations may be hesitant to share information that could be useful to prevent cyber threats as the disclosure of certain information could result in civil or criminal liability.
- **Targeted population** : Private organizations and corporations.
- **Goals of the policy** :
  The Cybersecurity Information Sharing Act of 2015 encourages the voluntary sharing of cyber-threat information and defensive cybersecurity measures between private organizations and the government in the goal of reducing the amount of cyber-attacks on American corporations.
- **Components of the policy** :
  - The Cybersecurity Information Sharing Act of 2015 (CISA) essentially authorizes private companies

to monitor, share and receive cybersecurity threat information and defensive measures with the government and other private entities without fear of civil or criminal liability.

- CISA ensures that companies sharing or receiving cyber threat indicators or defensive measures (any action that attempts to negatively affect an information system or countermeasure to protect such a system) are protected from liability, as long as it is for cybersecurity purposes. This means that these companies cannot be legally prosecuted for sharing cybersecurity information that would be illegal to share otherwise. Companies that share cyber threat information or defensive measures with other companies for cybersecurity purposes cannot be found guilty of violating U.S. antitrust laws or any federal, state or local privacy disclosure law under CISA.
- There are limitations to what information different entities can share and use. All entities under CISA may only monitor, share and receive threat information or defensive measures with the purpose of protecting or enhancing their cybersecurity or their partners' cybersecurity. All information shared and received must fit CISA's definition of "cyber threat indicator" or "defensive measure" to benefit from liability protection. Furthermore, CISA requires all information sharing entities to remove the personal information of individuals not concerned by the cyber threat. Specific concern is given to health, human resource, educational, financial and property ownership information as well as the information of children under the age of 13. These types of information have been identified by the Department of Homeland Security as being unlikely to be cyber threat indicators and requiring particular care when being submitted under CISA.
- The Department of Homeland Security (DHS) set up a server system called Automated Indicator Sharing (AIS) that facilitates the exchange of cyber threat indicators and defensive measures through public and private entities. The DHS, along with the Department of Justice, also released multiple guides to better explain the sharing and reception of cyber threat indicators through the AIS and other channels, such as Information Sharing and Analysis Centers or organizations that already share information with the DHS. These guides also provide clearer definitions of the terminology used in CISA and gives clear concrete examples of what is permitted and what is not.

• **Agents in charge** :

1) The US Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury and the Office of the Director of National Intelligence are charged with overseeing the correct implementation of CISA. One year after CISA's enactment, and once every two years thereafter, these departments must submit a report to Congress outlining and assessing the proper and timely use of CISA by federal and non-federal entities.
2) The Department of Homeland Security (DHS) is tasked with the initial reception of cyber threat indicators and defensive measures by the federal government. Once the information is

received by the DHS, it is then automatically shared with all federal departments previously mentioned. The National Cybersecurity and Communications Integration Center (NCCIC) is a DHS-led operation that operates the Automated Indicator Sharing (AIS) program.

- **Costs** :
  The Congressional Budget Office estimates that CISA will cost approximately USD 20 million from 2016-2020.
- **Sources of funding** : Department of Homeland Security (DHS)
- **Penalties** : No. CISA creates no legal obligation to share information; it is purely voluntary.
- **Incentives** :
  Companies that voluntarily share useful cyber-threat information with the government may receive information on better cyber-defence in return.
- **Challenges** :
  Many different people and organizations have opposed the bill both before and after its implementation.
  1) Democratic Senators Ron Wyden of Oregon and Mark Udall of Colorado voted against the bill in 2014, arguing that it "lacked adequate protections for the privacy rights of law-abiding Americans." (McNeal, 2014). When the bill was reintroduced in 2015, Wyden voted against CISA again in 2015, calling it a "surveillance bill" (Greenberg, 2015).
  2) Vermont Senator and ex-Presidential candidate Bernie Sanders also opposed the bill (Geller, 2015).
  3) Republican Senator Justin Amash of Michigan introduced a bill in January 2016, shortly after CISA's enactment, to repeal it, calling it the "worst anti-privacy law since the USA Patriot Act" (Bennet, 2016). He argued that the Cybersecurity Act was negotiated in secret by only a few members of Congress and tacked onto an extremely large omnibus to avoid criticism or challenge. He argues that most representatives likely did not even know they signed the act.
  4) Robyn Greene, privacy counsel of Open Technology Institute, criticized the bill in February 2015, shortly before it was reintroduced to the Senate. Greene argued that the type of language used in CISA might allow sharing of personal information beyond cybersecurity issues.
  5) The Center for Democracy in Technology (CDT) also opposed the bill. In March 2015, it wrote an open letter to Burr and Feinstein, signed by 27 civil organizations and 22 computer science experts. It suggested significant changes to the bill, such as using more precise language to define a cyber-threat indicator, as defined in the July 2012 Cybersecurity Bill.
  6) One of the organizations that signed the CDT open letter, the Electronic Frontier Foundation (EFF), is especially vocal about its disapproval of CISA. The EFF calls CISA a "privacy-invasive surveillance bill" and argues that it would give companies more power to obtain private

communications from users and disclose “threat data” to government without a warrant. Before CISA was signed, the EFF encouraged Americans to get in touch with their Senators to tell them to vote “no” to the bill.

7) Numerous online social media organizations and technology news outlets such as Twitter, Reddit, Yelp, Engadget, Upworthy and TechCrunch have also publicly condemned CISA before its implementation (Rogers 2015).

4. Implementation Information

- June 2014: *Democrat* Senate Intelligence Committee Chairman of California Dianne Feinstein releases draft version of the Cybersecurity Information Sharing Act of 2014 (CISA).
- July 2014: Senator Feinstein introduces CISA in the 113th Congress. CISA passes the Senate Select Committee on Intelligence but did not reach a full senate vote.
- March 2015: Republican Senator of North Carolina Richard Burr reintroduces CISA in the 114th Congress by combining the pre-existing bill CISA bill with another bill, the Cyber Threat Sharing Act of 2015. Bill passes Senate Select Committee on Intelligence.
- October 2015: Senate passes CISA.
- December 2015: President Barack Obama signs the Cybersecurity Information Sharing Act of 2015 (CISA) into law as part of the Cybersecurity Act of 2015.
- March 2016: Automated Indicator Sharing is operable.
- June 2016: Department of Homeland Security releases clearer sharing and reception guidelines.
- September 2025: CISA expires.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf

7. Publications

Abascal, M. A., Schindler, D. J., Archie, J. C., Jones, S. C., Crawford, G. E., Stout, A. L., & Naftalis, B. A. (2016). What You Need to Know About the Cybersecurity Act of 2015. *Latham &*

Watkins Client Alert Commentary. Retrieved from: https://www.lw.com/thoughtLeadership/lw-Cybersecurity-Act-of-2015

Evangelakos, J., & McIntosh, B. J. (2016, January 12). A Guide To The Cybersecurity Act Of 2015 - Law360. Retrieved August 19, 2017, from https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015

Jasper, S. E. (2017). U.S. Cyber Threat Intelligence Sharing Frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53–65. https://doi.org/10.1080/08850607.2016.1230701

Johnson, A. L. (2016). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation News & Comments: IV. Cybersecurity and Financial Institutions. *North Carolina Banking Institute*, *20*, 277–310.

Karp, B., S. Federal Guidance on the Cybersecurity Information Sharing Act of 2015. March 3rd, 2016. Retrieved from: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

Margulies, P. (2017). *Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy* (SSRN Scholarly Paper No. ID 2902212). Rochester, NY: Social Science Research Network. Retrieved from SSRN: https://papers.ssrn.com/abstract=2902212

Schwartz, A., Shah, S., MacKenzie, M., Thomas, S., Potashnik, T., & Law, B. (2017). Automating Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information With Other Companies or Organizations. *University of Michigan Journal of Law Reform*, *50*(4), 887–911.

Tran, J. L. (2016). Navigating the Cybersecurity Act of 2015 Symposium: Cyberwars: Navigating Responsibilities for the Public and Private Sector. *Chapman Law Review*, *19*, 483–500.

8. Media Articles

Bennett, C. Amash bill would repeal new cybersecurity law. January 14th, 2016. Retrieved from: http://thehill.com/policy/cybersecurity/265852-amash-bill-would-repeal-new-cybersecurity-law

Bing, C. Apple, Google and Friends Join Forces Ahead of Crucial CISA Decision. October 20th, 2015. Retrieved from: https://www.americaninno.com/dc/cisa-senate-vote-cybersecurity-information-sharing-act-congress/

Brandom, R. Congress is about to vote on a terrible new cybersecurity bill. July 19th, 2014. Retrieved from: https://www.theverge.com/2014/7/9/5881691/congress-will-vote-on-CISA-controversial-cybersecurity-bill

Brandom, R. Congress passes controversial cybersecurity bill attached to omnibus budget. December 28th, 2015. Retrieved from: https://www.theverge.com/2015/12/18/10582446/congress-passes-cisa-surveillance-cybersecurity

Caldwell, G. Why You Should Be Concerned About The Cybersecurity Information Sharing Act. February 7th, 2016. Retrieved, from: https://techcrunch.com/2016/02/07/why-you-should-be-concerned-about-cisa/

Cameron, D. Privacy groups rally to block controversial cybersecurity bill. March 5th, 2015. Retrieved from: https://www.dailydot.com/layer8/cisa-letter-intelligence-committee/

Center for Democracy & Technology. Letter to Senate Select Committee on Intelligence regarding CISA. March 2nd, 2015. Retrieved from: https://cdt.org/insight/letter-to-senate-select-cmte-on-cisa/

Comulada, J. The 2016 spending bill just passed. Good news: Funding for NASA. Bad news: CISA. December 18th, 2015. Retrieved from: http://www.upworthy.com/the-2016-spending-bill-just-passed-good-news-funding-for-nasa-bad-news-cisa

Chew, W. & Newby, T. G. The Cybersecurity Information Sharing Act of 2015: An Overview. October 24th, 2016. Retrieved from: http://www.lexology.com/library/detail.aspx?g=31bc698a-ec4d-4b9b-a8a9-46d893777a10

Electronic Frontier Foundation. Stop the Cybersecurity Information Sharing Act. Undated. Retrieved from: https://act.eff.org/action/stop-the-cybersecurity-information-sharing-act

Geller, E. Bernie Sanders is the only 2016 presidential candidate who opposes CISA. October 12th, 2015. Retrieved from: https://www.dailydot.com/layer8/bernie-sanders-cisa-senate-2016-presidential-candidates/

Greenberg, A. CISA Cybersecurity Bill Advances Despite Privacy Concerns. March 12th, 2015. Retrieved from: https://www.wired.com/2015/03/cisa-cybersecurity-bill-advances-despite-privacy-critiques/

Greenemeier, L. A Quick Guide to the Cybersecurity Bill Passed by the U.S. Senate. October 28th, 2015. Retrieved from: https://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/

Link, R. What You Need to Know About the Cybersecurity Information Sharing Act of 2015. October 10th, 2016. Retrieved from: http://www.isaca.org/cyber/cyber-security-articles/Pages/what-you-need-to-know-about-the-cybersecurity-information-sharing-act-of-2015.aspx?utm_referrer=

McNeal, G. S. Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee. July 9th, 2014. Retrieved from: https://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/

Petrasic, K., & Bornfreund, M. CISA Guidance Clarifies How to Share Cyber Threat Information… but Issues Remain. April 18th, 2016. Retrieved from: http://www.whitecase.com/publications/alert/cisa-guidance-clarifies-how-share-cyber-threat-information-issues-remain

Rogers, J. Twitter slams controversial cybersecurity bill. October 20th, 2015. Retrieved from: http://www.foxnews.com/tech/2015/10/20/twitter-slams-controversial-cybersecurity-bill.html

Rosenfeld, E. The controversial "surveillance" act Obama just signed. December 22, 2015. Retrieved from: http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html

Velazco, C. Budget bill heads to President Obama's desk with CISA intact. December 18th, 2015. Retrieved from: https://www.engadget.com/2015/12/18/house-senate-pass-budget-with-cisa/

Williams, K. B. Intel chairs slam "knee-jerk" opposition to cyber sharing bill. October 2nd, 2015. Retrieved from: http://thehill.com/policy/cybersecurity/255778-intel-chairs-slam-cisa-opponents

9. Documents

N/A

10. Related Law / Policies / Etc.

N/A

11. Keywords

Privacy Protection, Information Sharing, Private-Public Partnership, Cyber-Threat Data

12. Snapshot

- Targeted population: Public and private institutions
- Geographical scope: USA
- Policy type: Information sharing
- Status: Active

USA – National Institute of Standards and Technology (NIST) Cybersecurity Framework

1. Summary

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework) is a voluntary policy framework in the United States of America. Launched in 2014, the Framework addresses the growing cyber threat to critical infrastructure. It is aimed at the owners, operators and providers of both public and private critical infrastructure industries. The framework has three main components: the Framework Core, Framework Profiles and Implementation Tiers. Together, these pieces of the Framework help organizations determine their cybersecurity risk level and give them resources to rectify problem areas. Though heavily mentioned in the media and under constant scrutiny from stakeholders, the Framework has yet to be empirically evaluated.

2. Nature

Standardization and Accreditation

3. Policy's Description

- **Date** :
  - February 2013: Executive Order 13636 announces the development of the Cybersecurity Framework.
  - February 2014: Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity is released.
  - January 2017: Draft update Version 1.1 of the Framework is released.
- **Country** : United States of America
- **Geographical scope** :
  United States of America; however, other countries, such as Israel, Canada, the UK and Malaysia have modeled similar cybersecurity frameworks after the NIST Cybersecurity Framework.
- **Instigator** :
  United States Government (Obama Administration), under Presidential Policy Directive 21 (Critical Infrastructure Security and Resilience).
- **Targeted issue / situation** :
  The cyber threat to critical infrastructure is a growing and serious national security challenge for the U.S. Government. Government and industry must be equipped to deal with cyber threats as critical infrastructure increases in complexity and connectivity over time.

- **Targeted population** :

  Operators of critical infrastructure, stakeholders and members in government and industry, as well as users and innovators of cybersecurity solutions. In 2016, market research estimates that approximately 30% of U.S. organizations use the Framework.

- **Goals of the policy** :

  The Framework collaborates with stakeholders in government and industry to create a set of standards, methodologies, procedures, and processes that bring together policy, business, and technological approaches to deal with cyber risk and through voluntary consensus standards and best practices. It aims to end the fragmented approach to cybersecurity by providing a cohesive framework that can tie critical infrastructure together.

- **Components of the policy** :

  - The NIST Cybersecurity Framework is a voluntary approach to managing cybersecurity risk for critical infrastructure. It is made of three parts: the Core, the Profile and the Implementation Tiers.
  - The Core provides activities, references and guidance to achieve specific cybersecurity outcomes. The Core is divided into four parts: Functions, Categories, Subcategories and Informative References. There are five Core Functions: Identify, Protect, Detect, Respond and Recover. Each function is divided into categories, such as Asset Management for Identify or Mitigation in Respond. Categories are then divided into Sub-Categories and finally completed with Informative References to consult in order to achieve each function.
  - The Profile is an alignment of the Functions, Categories and Subcategories with the specificities of each organization. Every business has different requirements, resources and risk tolerance. Organizations can use Framework Profiles to describe their current state or target state of cybersecurity. There are no profile templates, so each organization can have a customized template for its needs.
  - The Tiers help an organization determine how it views cybersecurity risk and the processes that are in place to manage risk. There are four Tiers: 1 - Partial, 2 - Risk Informed, 3 - Repeatable and 4 - Adaptive. The Tiers describe an increasing amount of thoroughness in an organization's risk management. Though it is generally encouraged for Tier 1 organizations to progress to higher Tiers with time, other level Tiers may only feel the need to shift if it benefits their organization.
  - Furthermore, the NIST released the Baldrige Cybersecurity Builder, a self-assessment tool that aims to help organizations better understand just how effective their risk management efforts are and detect opportunities to improve.
  - Finally, the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community (C^3) Voluntary Program, which aims to encourage the adoption of the Framework. The C^3 Voluntary Program serves as a point of contact to help organizations who are

interested in the Framework and to receive feedback from those who already use it.

- **Agents in charge** :

1) The U.S. Department of Commerce National Institute of Standards and Technology (NIST) is a non-regulatory federal agency that is known to partner with industry, other government agencies, and academia to address critical national issues. The NIST is in charge of the development, implementation and maintenance of the Cybersecurity Framework. It convenes Framework stakeholders, solicits advice and recommendations and updates the Framework when necessary.
2) The Department of Homeland Security is responsible for ensuring the safety and protection of the USA at many different levels. Executive Order (EO) 13636, directs the Departments of Homeland Security to reinforce use of the NIST Cybersecurity Framework and participation in the C^3 Voluntary Program.

- **Costs** : Unknown
- **Sources of funding** : Unknown
- **Penalties** : N/A
- **Incentives** :

Although the Framework is technically voluntary, there have been reports that certain organizations require mandatory compliance to the Framework to maintain insurance. Because the Framework is considered the “standard” by many, if an organization is found not to comply it may face penalties during audits or insurance claims (Gyenes, 2013; Shen, 2014; Verry, 2014).

- **Challenges** : N/A

4. Implementation Information

- February 2013: Executive Order 13636 announces the development of the Cybersecurity Framework; NIST issues a Request for Information (RFI) in the Federal Register about current risk management, use of frameworks, standards, guidelines and best practices as well as specific industry practices.
- February 2014: Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity is released. DHS launches Critical Infrastructure Cyber Community (C^3).
- January 2017: Draft update Version 1.1 of the Framework is released.
- March 2017: Version 1.0 of The Baldrige Cybersecurity Excellence Builder launched.

5. Evaluation

- **Existence of an evaluation** : No

- **Evaluation type** : N/A
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

6. URL

https://www.nist.gov/cyberframework

7. Publications

Dimensional Research. (2016, March). Trends in Security Framework Adoption: A Survey of IT and Security Professionals. Available at Tenable: http://static.tenable.com/marketing/tenable-csf-report.pdf

Hiller, J. S., & Russell, R. S. (2017). Privacy in Crises: The NIST Privacy Framework. *Journal of Contingencies and Crisis Management, 25*(1), 31–38. Available at Wiley Online Library: https://doi.org/10.1111/1468-5973.12143

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. *Texas International Law Journal, 50*, 305–356. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631

Shackelford, S. J., Russell, S., & Kuehn, A. (2017). Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector. In *Ethics and Policies for Cyber Operations*, 115–137. Available at Springer: https://doi.org/10.1007/978-3-319-45300-2_8

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer, 10*(4), 16. Available at Mayer Brown: https://www.mayerbrown.com/The-NIST-Cybersecurity-Framework-Overview-and-Potential-Impacts/

Teodoro, N., Gonçalves, L., & Serrão, C. (2015). NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements. In *Proceedings of 2015 IEEE Trustcom/BigDataSE/ISPA*, 418–425. Available at IEEE Xplore: https://doi.org/10.1109/Trustcom.2015.402

8. Media Articles

Bernard, M. E. S. NIST Cybersecurity Framework review - Management System GAPS. September 23rd, 2014. Retrieved from

https://www.linkedin.com/pulse/20140923034306-12861716-nist-cybersecurity-framework-review-management-system-gaps

Brown, J. Analyzing proposed updates to the NIST Cybersecurity Framework. April 14th, 2017. Retrieved from http://blogs.ca.com/2017/04/14/analyzing-proposed-updates-nist-cybersecurity-framework/

Brumfield, C. NIST Cybersecurity Framework is Good and Bad, Experts Say. August 21st, 2014. Retrieved from http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html

Christensen, D. 4 Insights on New Baldrige Cybersecurity Excellence Builder Assessment. April 5th, 2017. Retrieved from https://www.linkedin.com/pulse/4-insights-new-baldrige-cybersecurity-excellence-builder-hanno-ekdahl

Davis, R. H. Reactions to NIST's Final Cybersecurity Framework – The Good and the Bad (but no ugly). February 16th, 2014. Retrieved from https://thesecuretimes.wordpress.com/2014/02/16/reactions-to-nists-final-cybersecurity-framework-the-good-and-the-bad-but-no-ugly/

Drolet, M. Learn What NIST's Cybersecurity Framework Can Do For You. June 6th, 2017. Retrieved from http://www.networkworld.com/article/3199968/network-security/learn-what-nists-cybersecurity-framework-can-do-for-you.html

Durbin, K. Demystifying the NIST Cybersecurity Framework for Healthcare. May 12th, 2017. Retrieved from http://www.symantec.com/connect/blogs/demystifying-nist-cybersecurity-framework-healthcare

Eggers, M. J. (2014, February 12). Cybersecurity Framework: A Good Start, But More Work Ahead. February 12th, 2014. Retrieved from https://www.uschamber.com/above-the-fold/cybersecurity-framework-good-start-more-work-ahead

Francis, M. The future of the NIST Cybersecurity Framework. April 25th, 2016. Retrieved from https://iapp.org/news/a/the-future-of-the-nist-cybersecurity-framework/

Friedman, S. What's next for NIST cybersecurity framework? May 16th, 2017. Retrieved from https://gcn.com/articles/2017/05/16/nist-cybersecurity-framework.aspx

Grossman, S. NIST's cybersecurity framework is changing – what you should know. March 31st, 2017. Retrieved from https://gcn.com/articles/2017/03/31/cybersecurity-framework-revisions.aspx

Guinn, J II. Why you should adopt the NIST Cybersecurity Framework. May, 2014. Retrieved from http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Intrinium. NIST Cybersecurity Framework Adoption or Bust! April 7th, 2017. Retrieved from https://intrinium.com/nist-cybersecurity-framework-adoption-or-bust/

Kahn, R. The Increasing Popularity of the NIST Cybersecurity Framework. October 4th, 2016. Retrieved from https://blog.tanium.com/increasing-popularity-nist-cybersecurity-framework-2/

Langner, R. What a cyber security framework for industrial control needs to look like. September 4th, 2013. Retrieved from https://www.langner.com/2013/09/what-a-cyber-security-framework-for-industrial-control-systems-needs-to-look-like/

McKay, A. Lessons from the NIST Cybersecurity Framework. October 5th, 2016. Retrieved from https://blogs.microsoft.com/microsoftsecure/2016/10/05/lessons-from-the-nist-cybersecurity-framework/

Nicholas, P. NIST Cybersecurity Framework: Building on a foundation everyone should learn from. June 7th, 2017. Retrieved from https://blogs.microsoft.com/microsoftsecure/2017/06/07/nist-cybersecurity-framework-building-on-a-foundation-everyone-should-learn-from/

National Institute of Standards and Technology. Cybersecurity "Rosetta Stone" Celebrates Two Years of Success. February 18th, 2016. Retrieved from https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success

National Institute of Standards and Technology. NIST Releases Baldrige-Based Tool for Cybersecurity Excellence. September 15th, 2016. Retrieved from https://www.nist.gov/news-events/news/2016/09/nist-releases-baldrige-based-tool-cybersecurity-excellence

National Institute of Standards and Technology. NIST Releases Update to Cybersecurity Framework. January 10th, 2017. Retrieved from https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework

Otto, G. Workshop plots evolution of NIST Cybersecurity Framework. April 7th, 2016. Retrieved from https://www.fedscoop.com/nist-workshop-plots-evolution-of-cybersecurity-framework/

Siegel. Voluntary But Valuable: Using NIST's New Cybersecurity Framework. February 20th, 2014. Retrieved from http://cyberlawmonitor.com/2014/02/20/voluntary-but-valuable-using-nists-new-cybersecurity-framework/

Tenable. NIST Cybersecurity Framework Adoption Linked to Higher Security Confidence According to New Research from Tenable Network Security. March 29th, 2016. Retrieved from

https://www.tenable.com/press-releases/nist-cybersecurity-framework-adoption-linked-to-higher-security-confidence-according

Tracy, R. P. Unlocking the Power of NIST's Cybersecurity Framework. April 28th, 2017. Retrieved from http://www.nextgov.com/technology-news/tech-insider/2017/04/unlocking-power-nists-cybersecurity-framework/137434/

Tripwire. ISA Outlines Criteria to Evaluate NIST Cyber Security Framework. February 6th, 2014. Retrieved from https://www.tripwire.com/state-of-security/latest-security-news/isa-outlines-criteria-evaluate-nist-cyber-security-framework/

Verry, J. Why the NIST Cybersecurity Framework Isn't Really Voluntary. February 25th, 2014. Retrieved July 18, 2017, from https://www.pivotpointsecurity.com/blog/nist-cybersecurity-framework/

9. Documents

PPD-21
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Executive order 13636
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

10. Related Law / Policies / Etc.

Cybersecurity Enhancement Act of 2014 (Public Law 113-274)

11. Keywords

Framework, Risk Management, Voluntary Measures

12. Snapshot

- Targeted population: Critical infrastructure, government, industry
- Geographical scope: USA
- Policy type: Standardization and Accreditation
- Status: Active

USA – National Institute of Standards and Technology CyberSeek (NIST CYBERSEEK)

1. Summary

CyberSeek is an American cybersecurity career information resource aiming to close the cybersecurity skill gap existing in the United States of America. It was created by the National Initiative for Cybersecurity Education (NICE) led by the National Institute of Standards and Technology (NIST), CompTIA and Burning Glass Technologies in November 2016. It includes two interactive tools: a heat map and a career pathway. The heat map provides information on job supply and demand, while the career pathway helps illustrate different career opportunities. The resource received a three-year federal grant and operates online, serving all 50 states of the USA.

2. Nature

Workforce Development

3. Policy's Description

- **Date** :
  November 2016: NIST launched the Cyberseek tool at the 2016 NICE Conference in Kansas City, Missouri.
- **Country** : United States of America
- **Geographical scope** : United States of America
- **Instigator** :
  NICE is a partnership between the public and private sector creating a network of cybersecurity education and training. NICE is led by NIST, a non-regulatory agency of the U.S. Department of Commerce that promotes industrial and scientific innovation. Cyberseek was created by a non-profit trade association for IT professionals called CompTIA, which partnered with Burning Glass Technologies, a labour market analytics firm.
- **Targeted issue / situation** :
  This program seeks to address the cybersecurity skills gap and the shortage in cybersecurity workers in the United States. According to Burning Glass (Nov 1, 2006), "there are 128,000 positions for Information Security Analysts, but only 88,000 workers currently employed in those positions—a talent shortfall of 40,000 workers for cybersecurity's largest job."[15]

[15] http://burning-glass.com/cyberseek-map-solving-cybersecurity-skills-gap/

- **Targeted population** :
  - Employers curious about the scale, cost and demand of the cybersecurity workforce in their area or across the country.
  - Educators, Career and Guidance Counselors & Training Providers interested in including information on cybersecurity jobs in their programs.
  - Students, Job Seekers & Current Workers interested in learning more about the demand and skills needed to advance a career in cybersecurity.
  - Policy Makers who need to stay informed on community workforce shortages and demand.
- **Goals of the policy** :

  CyberSeek provides detailed information about supply and demand in the cybersecurity job market to help close the skills gap. The tool is designed to facilitate cybersecurity job searching. It makes it easier for job seekers to find openings and for employers to identify skilled workers.
- **Components of the policy** :

  This program operates an interactive online resource for cybersecurity career information. People who are curious about the cybersecurity workforce in their area can access cyberseek.org to obtain more information. The online resource has two primary components:

  1) An interactive cybersecurity supply/demand heat map. This analytics tool uses data collected by Burning Glass Technologies and the Bureau of Labor Statistics. It determines job availability and fulfillment per metro area or per state. Each geographical region is assigned a colour code, like a heat map, based on: cybersecurity job openings, supply of workers, supply/demand ratio and geographical concentration;
  2) An interactive Career Pathway. The Career Pathway shows different career paths in cybersecurity. The Career Pathway details: the average salary; common job titles; requested education, certifications and skills; total job openings and common NICE framework categories of each career path.

  It is important to note that this resource does not act as a broker between those posting a job opening and someone wishing to apply. It does not provide access to the job postings. For example, the heat map may mention the *number* of job openings in a city, but does not provide access to the job openings themselves. It more simply provides information about the state of the cybersecurity workforce in a certain area. The resource itself does not take any active steps to close the cybersecurity skills gap. Instead, it exists as collection of online tool that can be consulted by those in need of information.
- **Agents in charge** :
  1) No entities were created. The program was created by NICE/NIST, CompTIA, and Burning Glass Technologies. CompTIA is a non-profit trade association that offers training and

certification for Information Technology (IT) professionals. Burning Glass Technologies is an analytics software company specialized in labour market information.

2) NICE/NIST were responsible for funding and announcing the resource. They do not seem to be otherwise engaged in the development of the resource but this is unclear.
3) It is not precisely established how CompTIA and Burning Glass Technologies independently contribute to the resource.
4) CompTIA states that CyberSeek's "data come from various certifying bodies, including CompTIA, ISACA, ISC2 and IAPP as well as Burning Glass, which uses technology deliver insight on workforce and economic development, career exploration and counseling, and match people with jobs."[16]

- **Costs** :

  The first-year grant was USD 249,000 and the program received USD 110,000 for its second year.

- **Sources of funding** :

  The NICE, led by the NIST, funded the development of the tool with a three-year grant.

- **Penalties** : N/A
- **Incentives** : N/A
- **Challenges** : No

4. Implementation Information

- November 2016: NIST announced Cyberseek tool at the 2016 NICE Conference in Kansas City, Missouri.
- It is not clear how frequently the data is updated.
- Future plans: CompTIA mentioned at launch that they plan to include data from other certifying bodies.

5. Evaluation

- **Existence of an evaluation** : No
- **Evaluator** : N/A
- **Methodology** : N/A
- **Outcomes** : N/A

[16] https://certification.comptia.org/it-career-news/post/view/2016/11/01/cyberseek-tracks-explosion-in-cybersecurity-demand

6. URL

http://cyberseek.org/

7. Publications

N/A

8. Media Articles

Bur, J. New Cybersecurity Job Search Tool Features Interactive Map. November 1st, 2016. Retrieved from https://www.meritalk.com/articles/new-cybersecurity-job-search-tool-features-interactive-map/

Burning Glass. Cyberseek: A Map to Solving the Cybersecurity Skills Gap. November 1st, 2016. Retrieved from http://burning-glass.com/cyberseek-map-solving-cybersecurity-skills-gap/

Executive Gov. NIST Unveils Online Tool to Support Cyber Job Seekers & Employers. November 2nd, 2016. Retrieved from http://www.executivegov.com/2016/11/nist-unveils-online-tool-to-support-cyber-job-seekers-employers/

Francis, A. Security Central: Webcams Recalled in Cyber-attack Aftermath, NIST Announces CyberSeek Tool. November 3rd, 2016. Retrieved from http://thevarguy.com/network-security-and-data-protection-software-solutions/security-central-webcams-recalled-cyber-atta

Lange, M. CyberSeek Tracks Explosion in Cybersecurity Demand. CompTIA. November 1st, 2016. Retrieved from https://certification.comptia.org/it-career-news/post/view/2016/11/01/cyberseek-tracks-explosion-in-cybersecurity-demand

National Institute of Standards and Technology. NIST Announces CyberSeek, An Interactive Resource for Cybersecurity Career Information. November 1st, 2016. Retrieved from https://www.nist.gov/news-events/news/2016/11/nist-announces-cyberseek-interactive-resource-cybersecurity-career

O'Neill, P. H. How to make sense of the wide open cybersecurity job market. November 1st, 2016. Retrieved from https://www.cyberscoop.com/cyberseek-comptia-nice-cybersecurity-job-market/

Palic, J. CompTIA Introduces Cyberseek for Job Seekers. February 15th, 2017. Retrieved from https://www.onlc.com/blog/comptia-introduces-cyberseek-job-seekers/

Dark Reading. Tool for Cybersecurity Job Hunters Launched. November 2nd, 2016. Retrieved from

http://www.darkreading.com/careers-and-people/tool-for-cybersecurity-job-hunters-launched/d/d-id/1327369

Employment & Training Administration (ETA). U.S. Department of Labor. NIST Introduces New Cybersecurity Job Search Tool; Features Employment Opportunities by State and Locality, Potential Career Pathways, Interactive Map. Retrieved from https://www.doleta.gov/usworkforce/whatsnew/eta_default.cfm?id=6793

9. Documents

N/A

10. Related Law / Policies / Etc.

N/A

11. Keywords

Cybersecurity Workforce, Skills Gap, Job-Search Resources

12. Snapshot

- Targeted population: Employers, Educators, Career and Guidance Counselors & Training Providers, Students, Job Seekers & Current Workers, Policy Makers
- Geography: United States of America
- Policy Type: Workforce Development
- Status: Active

3 Conclusion

As the 24 policy summaries presented in this report make it abundantly clear, the term cybersecurity is used to describe a broad range of government interventions that vary greatly in terms of goals; implementation and delivery strategies; levels of coerciveness; types of engagement with the private sector; and outcomes. However, what unites most of them is the unfortunate scarcity of 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 how it lends itself to the automated collection of performance indicators and metrics. Given the considerable investments being made by governments and organisations to improve their cybersecurity, it is concerning that there is not more efforts being undertaken to establish with scientific rigour the policies and programs that are delivering measurable improvements to the cybersecurity of our digital ecosystem. In our limited sample, less than one third of the reviewed policies have been evaluated, and not all of those independently.

Faced with a similar challenge, other policy domains such as public health, education and criminal justice have developed policy surveillance methodologies to better track how complex social issues and risk factors are being addressed by local and national governments. The tools and platforms that are associated with the policy monitoring approach facilitate knowledge transfers, cross-jurisdictional comparisons and enable evidence-based interventions. We have outlined in this report the main features of a diversified sample of existing policy monitoring tools and how they could be applied to the field of cybersecurity, including the specific challenges that would need to be met.

Several cyber capacity, readiness or maturity indexes have already been developed by international organizations and think-tanks. Their common denominator is a focus on countries considered at an aggregate level rather than on distinct cybersecurity policies. The limitation of this approach is that it prevents a more granular analysis of policy successes and failures.

Through the systematic description of a diversified sample of 24 cybersecurity policies, we have attempted to develop a methodology that could be used to develop a much larger and more comprehensive directory listing of existing policies, their features and their outcomes. To achieve this, an online platform providing search functionalities would represent a logical next step. The 24 policies outlined in this report could be transferred to the platform and new summaries would then be added regularly. Specific types of interventions or countries could be prioritized to focus

on policy innovation clusters. Finally, the platform would need to increase its profile and reach out to researchers and policy-makers through a well-targeted communications strategy.

We are aware that this is an ambitious goal that will require the development of a large-scale collaboration network involving researchers, policy-makers and volunteers from all over the world. The contributors who will feed the database of policies will also need to master the local languages in which these policies are drafted, implemented, challenged and evaluated, to avoid the reductionist trap of an over-reliance on English-language documents.

Despite these hurdles, we are convinced that creating such a Cybersecurity Policy Observatory and making its data publicly available and easily searchable would be extremely beneficial in advancing our collective capacity to respond to online harms.

4 References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., and Savage, S. (2013). Measuring the cost of cybercrime, in R. Böhme (ed.), *The economics of information security and privacy*, Springer, New York, pp. 265-300.

Burris, S., Wagenaar, A., Swanson, J., Ibrahim, J., Wood, J., and Mello, M. (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 Ramanathan T. (2016). Policy surveillance: A vital public health practice comes of age, *Journal of Health Politics, Policy and Law*, 41(6): 1061-1083.

Chriqui, J., O'Connor, J., and Chaloupka, F. (2011). What gets measured, gets changed: Evaluating law and policy for maximum impact, *The Journal of Law, Medicine & Ethics*, 39(1): 21-26.

CSE (2017). *Cyber threats to Canada's democratic process*, Communications Security Establishment, Ottawa.

CSIS (2014). *Net losses: estimating the global cost of cybercrime*, Center for Strategic and International Studies, Washington DC.

Cybersecurity Ventures (2017). *Cybersecurity Market Report*, Cybersecurity Ventures, Menlo Park, available online at https://cybersecurityventures.com/cybersecurity-market-report/.

Duckett, C. (2016). Budget 2016: Australian Cyber Strategy implementation broken out, *ZDNet*, available online at http://www.zdnet.com/article/budget-2016-australian-cyber-strategy-implementation-broken-out/.

Dutton, W. H., Creese, S., Shillair, R., Bada, M., and Roberts, T. (2017). Cyber security capacity: Does it matter?, *Quello Center Working Paper No. 2938078*, available online at 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, European Commission, Brussels, available online at http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

Gandel, S. (2015). Lloyd's CEO: Cyber attacks cost companies $400 billion every year, *Fortune*, available online at 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, Gartner, Sydney, available online at http://www.gartner.com/newsroom/id/3784965.

Hathaway, M. (2013). *Cyber Readiness Index 1.0*, Hathaway Global Strategies LLC, Washington DC, available online at http://www.belfercenter.org/sites/default/files/legacy/files/cyber-readiness-index-1point0.pdf.

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., and Spidalieri, F. (2015). *Cyber readiness index 2.0 - A plan for cyber readiness: A Baseline and an index*, Potomac Institute for Policy Studies, Washington DC.

ITU (2017a). *Global Cybersecurity Index (GCI) 2017*, International Telecommunications Union, Geneva.

ITU (2017b). *Index of cybersecurity indices*, International Telecommunications Union, Geneva.

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

Osborne, G. (2015). *Chancellor's speech to GCHQ on cyber security*, HM Treasury, London, available online at https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

Presley, D., Reinstein, T., and Burris, S. (2015). Resources for policy surveillance: A report prepared for the Centres for Disease Control and Prevention Public Health Law Program, *Temple University Legal Studies Research Paper No. 2015-09*, available online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567695.

The White House (2016). *Middle Class Economics: Cybersecurity*, The White House, Washington DC, available online at https://obamawhitehouse.archives.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity.pdf.

WEF (2017). *The global risks report 2017: 12th edition*, World Economic Forum, Geneva.

Zurich (2014). *Risk nexus - beyond data breaches: global interconnections of cyber risk*, Zurich Insurance Company, Zurich.

5 Annex 1: Coding Framework (Guidelines)

1. Summary

Program summary: sums up the main points of this note.

100 words maximum.

2. Nature

What is the main topic of the policy? Choose one subject :

- Public Awareness
- Capacity Building
- Education and Workforce Development
- Innovation & R&D
- Information Sharing
- Public-private Partnerships
- Regulation & Legislation
- Privacy Protection
- Standardization and Accreditation
- Law Enforcement and Crime Prevention
- Incentives and Nudging

3. Policy's Description

- **Date** :

  Implementation or date the program became effective.

  Format: Month / Year (i.e.: July 2017).

- **Country** : Where was the policy adopted?

- **Geographical scope** :

  Where does it apply?

  Is the policy local, national or international?

- **Instigator** : Who designed this program (group, organism, ministry…)?

- **Targeted issue / situation** : What is the issue being addressed by the program?

- **Targeted population** :

  What is the population targeted by the program (public organizations, companies, end users…)?

- **Goals of the policy** :

  What is the main aim of the policy?

What are the principal goals of the policy?

- **Components of the policy** :
  How is the policy implemented in practice?
  Describe the various components of the policy and how they are connected with the goals.
- **Agents in charge** :
  What are the organizations in charge of implementing the policy?
  Was an entity created to implement the policy? If yes, outline its structure.
  If there is more than one organizations, clarify the role of each. Who's in charge of what? How do they collaborate?
- **Costs** : How much does the policy cost to implement?
- **Sources of funding** :
  What organization or agency is funding the program?
  If there are several funding sources, provide detailed information on each partner's contribution.
- **Penalties** :
  Does the policy introduce a penalty / punishment / sanction as an enforcement mechanism? If yes, which one?
- **Incentives** :
  Does the policy introduces or relies on economic incentives?
  If yes, which ones?
- **Challenges** :
  Are there challenges raised against the policy by opposing groups?
  If yes, which ones (opponents, implementation hurdles…)?

4. Implementation Information

Has the policy been implemented?
Where? When?
List the stages.

5. Evaluation

- **Existence of an evaluation**
  Was the policy evaluated?
  Yes / No
- **Evaluation type** :
  Classify the type of evaluation (desktop, surveys, interviews, RCTs…).
  List the sources.

- **Evaluator** : Who performed the evaluation?
- **Methodology** : Describe the methodology used to perform the evaluation.
- **Outcomes** :
  What were the results of the evaluation?
  If applicable: how were the policy outcomes measured?

6. URL

URL of the policy's website.

7. Publications

Scientific articles published about the policy.
Reference format: Author, Year, Title, *Source* (name of the Journal / Conference / Rewiew), *Vol.*(Issue), Pages, URL.

8. Media Articles

Links to media articles referring to the policy.
Reference format: Author, Title, Date, URL.

9. Documents

List here all relevant documents produced by the policy's implementers: for example, links to downloadable qualitative and quantitative information related to the program.

10. Related Law / Policies / Etc.

List other policies from the database that adopt a similar approach.

11. Keywords

List Keywords for This Policy (Will Be Searchable Online).

12. Snapshot

A policy snapshot will be added to the webpage when the database is ported online, with bullet points enabling the reader to quickly filter policies based on key features such as:
- Targeted population
- Geographical scope
- Policy type
- Status (active, inactive)

Design Framework for the Creation of a Cybersecurity Policy Observatory

First Published in December 2017
Printed in Seoul, Republic of Korea