Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

An intelligence, economic, political, and technological cost/benefit analysis of cyber surveillance techniques

Jonathan Berliner

September 9, 2014

Report GW-CSPRI-2014-4

Support for this research was provided through a grant from the Centers & Institutes Facilitating Fund (CIFF) of the Office of the Vice President for Research of the George Washington University

Table of Contents

1. INTRODUCTION

1.1. Goal of the Model

The goal of this model is to increase transparency and understanding in evaluating surveillance techniques, assessing the effects of those techniques, and exploring options for optimally deploying surveillance to satisfy as many stakeholders as possible with the most utility. This makes explicit the priorities of stakeholders and allows policymakers to move forward on suggesting solutions. The results will be useful for policymakers, data privacy officers, systems engineers, programmers, economists, researchers, advocates, and their agents such as attorneys.

1.2. Significance of the Model

The emerging international discussion on surveillance has suffered from a surfeit of polarized opinions and a lack of good data and models to understand the complex question. Some politically-oriented actors in this space seem to have staked out extreme positions, suggesting that either open-ended surveillance is *absolutely* essential for national security or that complete privacy is *absolutely* essential for maintaining freedom. These two polarized sides see the solution to this issue as either eliminating surveillance altogether or leaving surveillance to the discretion of unregulated professionals. Neither allows for a more nuanced view of data collection and use that acknowledges "surveillance" as a large set of activities with different types of impacts on different stakeholders.

To have both security (via surveillance) and privacy requires better tools to properly analyze and evaluate policy options. This project develops an improved assessment mechanism that incorporates the views of more stakeholders than have traditionally been heard. This model articulates the various effects of various surveillance techniques based on the perspectives of various stakeholders. From this, analyses will emerge that addresses concerns for most or all stakeholders, and an analysis tool will be built to facilitate this result.

1.3. Why is this Solution Valid?

This approach bypasses the intense sensitivities related to national security, safety, and privacy, in favor of a rational approach that highlights areas of agreement and disagreement. By explicitly acknowledging differing subjective valuations, some measure of objectivity through careful classification is introduced.

1.4. Summary of Methodology

This paper includes both a theoretical model and an instantiation of it in a spreadsheet[1]. The model is represented as a 3-dimensional matrix (Figure 1) with surveillance techniques, tools, and programs along one axis, effects impacted by these techniques on a second axis, and stakeholders (such as national security agencies, diplomats, privacy advocates, media, and others) along the third axis.

[1] This spreadsheet is available at:

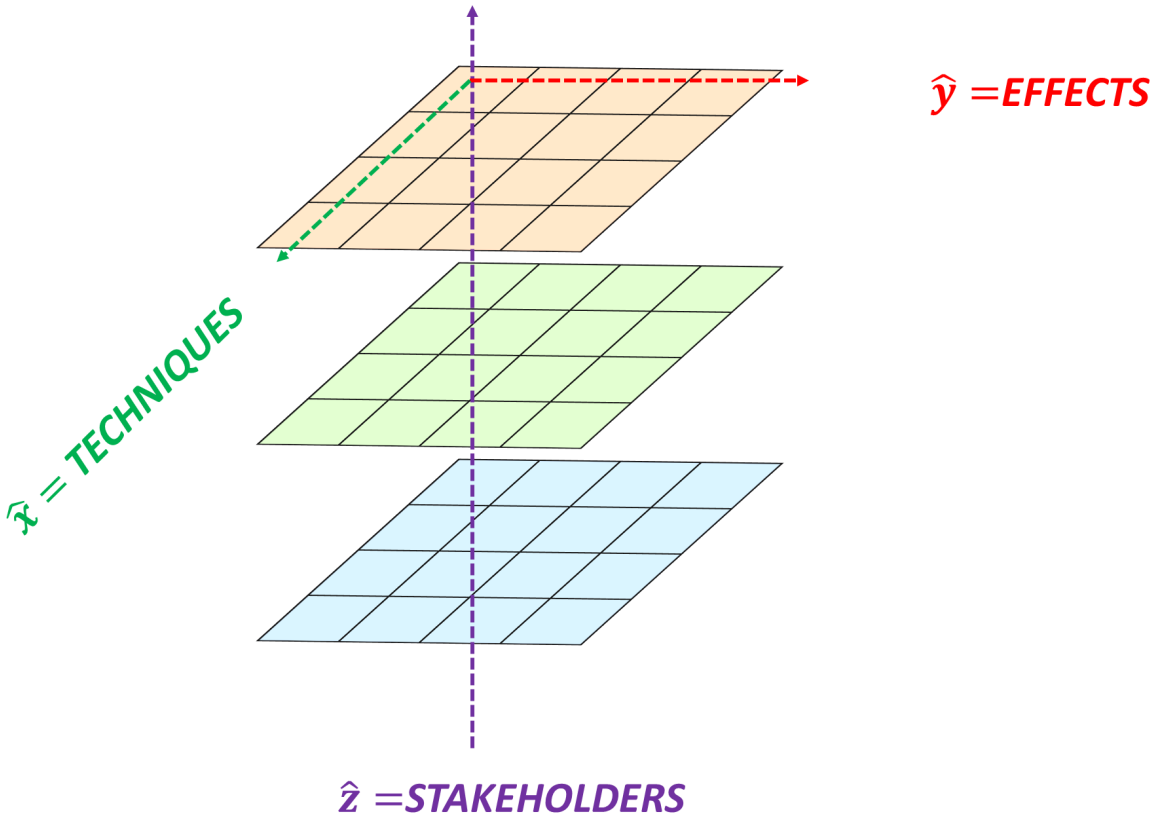


Figure 1 - 3D Matrix portraying multi-dimensional analysis of surveillance technique, effects, and stakeholders.

Each cell within this rectangular prism will receive a score based on how a specific surveillance technique induces a specific effect as perceived by a specific stakeholder. Once each of these inputs is provided, specific issues can be examined in detail with a goal of mitigating or eliminating the concerns of many, if not all, stakeholders. Figure 2 illustrates this in more detail.

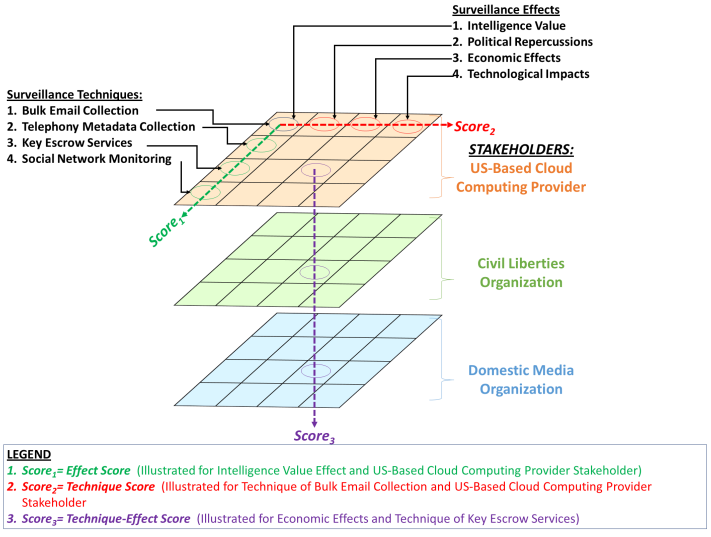


Figure 2 – Detailed illustration of cubic model, including sample details.

1.5. Rigor of the Model

The rigor of the model can be assessed in both its quantitative output and its process. As far as the quantitative output of the model, **users should not read the numerical results as being rigorous or corresponding to another standard effect of any kind**, whether it would be U.S. Dollars, bytes, or percentage points in the polls. *All of the model inputs were purely subjective*. Additionally, the techniques and effects that are included in this model are only a sample of the full population of surveillance techniques and effects in use today.

However, this model is still a significant contribution to the study of surveillance and intelligence because it yields interesting numerical results and this process is novel to the field. While much of the media during the height of the Snowden leaks may have focused on bulk data collection, the model indicated that Hardware Exploitation, Defeating Tor, and Inefficiencies of Standards may be among the most significant techniques and effects in the study of surveillance policy, and those are discussed in greater detail in that section. Notice that the discussion surrounds the qualitative implications of these results, not the derivative quantitative results from the specific numerical scores.

The rigor of the model's process is strong. Even though I believe that this process is novel for this kind of assessment of a surveillance agency, it reflects the complicated realities of surveillance policy, which is a multi-dimensional endeavor. This model implies a 4+ dimensional analysis, involving **techniques, effects, weights,** and **stakeholders**. While the process is flexible, it also allows minimal setup if a user merely wants to tweak any of the aforementioned dimensions.

The output of the model is very instructive:

- A ***Cumulative Surveillance Score*** which indicates the overall impact of a surveillance policy.
- ***Weighted*** and ***Unweighted Scores*** for each technique and effect's impact.
- Color-coding of cells immediately indicates the impact and extent of impact for hundreds of cells.
- Multi-dimensional linear analysis is simplified into fewer values.
- Users can immediately tell which techniques or effects were outliers in the analysis.
- **Standard Deviations** within each technique and effect indicate if a given technique or effect's score is due to a general impact of the technique or effect or just a few outliers.
- Scales are all rebalanced to the standard 1-5 scale to maintain consistency.

2. OPERATION OF MODEL

More details can be found in Appendix A.

2.1. Input Components of Model

The model consists of the following input components, which each represent a different dimension in the cubic model:

1. **Techniques**: Surveillance techniques are methods used by surveillance agencies for surveillance. They may be covert, overt, involve sabotage or not, involve personal property or not, and involve standards or not. I categorize them into (1) Standards Subversion (2) Collaborating with Industry (3) Defeating Cyber Security (4) Direct Attacks on Systems.
2. **Effects:** Surveillance effects are ways in which surveillance affects society and individuals. I categorize them into (1) Performance Effects (2) Economic Effects (3) Political Effects (4) Technological Effects

3. **Stakeholders:** Stakeholders are entities with biases, positions, or preferences staked out on which surveillance techniques or surveillance effects are important or unimportant for them. These values are also expressed as **Weights.**

2.2. Relational Inputs of Model

The relationship between **Techniques** and **Effects** is represented by two values:

1. **Likelihood –** How likely or strong the given **Technique** will induce a given **Effect.**
2. **Impact –** How positive or negative this effect inducement would be.

These values may vary by **Stakeholder**. They are multiplied together to provide an **Expected Impact** value which represents the eventual total positive/negative **impact** of an **effect** as induced by a **technique**.

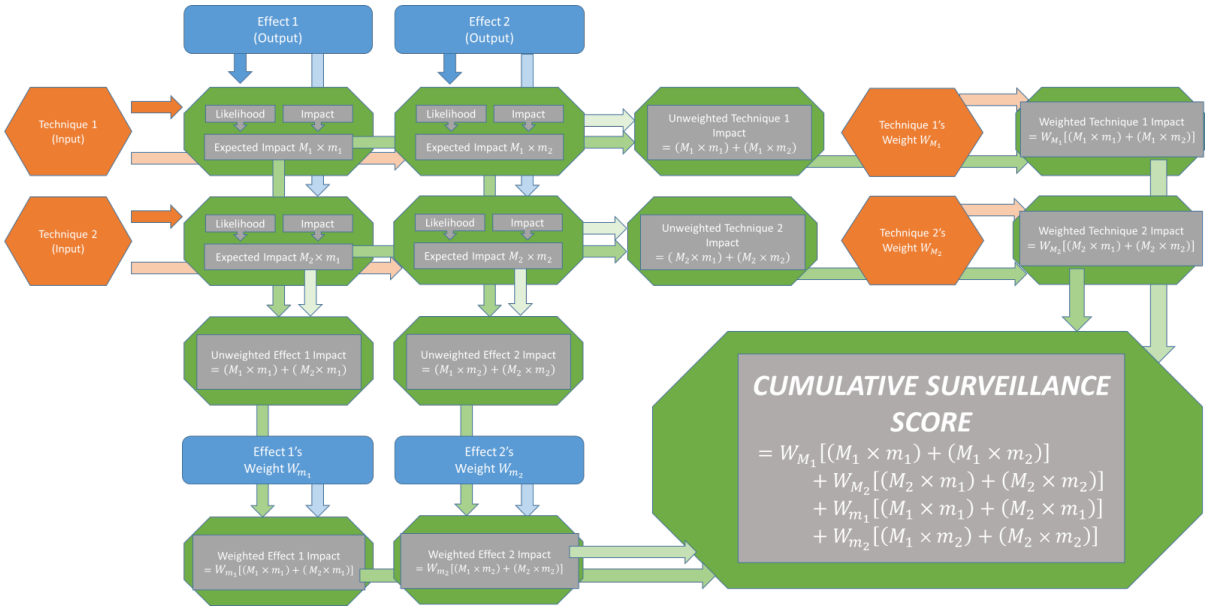
The **Expected Impacts** of each **Technique** and **Effect** are added up and multiplied by their corresponding **Technique/Effect Weight** to provide a **Weighted Technique/Effect Score**, indicating how impactful a given **Technique** or **Effect** is.

2.3. Cumulative Score

The **Cumulative Surveillance Score** is a sum of all of the **Weighted Technique/Effect Scores**. It represents the magnitude of a surveillance system's **Techniques** and **Effects** in terms of how positive or negative they are. In other words, a balanced distribution of positive and negative effects will yield a little-effect result.

Figure 3 is a graphical schematic of how the model functions in a simple 2-input, 2-output example, with simplified mathematical expressions. It is explained in greater detail in Appendix A.

Figure 3 – Graphical Schematic of Model (2-Input, 2-Output Example)



3. SURVEILLANCE TECHNIQUES CONSIDERED

3.1. GENERAL SURVEILLANCE TECHNIQUES

3.1.1. Bulk Collection of Personal Communications

This technique involves collecting as much data as possible, generally by tapping into primary communications channels or collaborating with the private sector directly. This data may involve emails, phone calls, cloud storage, messages, and a broad array of services provided by communications and Internet companies.

3.1.2. Hardware Exploitation

Surveillance can also be conducted by either exploiting computers directly or using sophisticated hardware techniques to conduct surveillance on individual machines. This can be done at the premises of the manufacturer, the target, or in between.

3.2. STANDARDS SUBVERSION

3.2.1. Weakening Public Use Cryptographic Ciphers

Weakening cryptographic ciphers is necessary for a surveillance agency primarily for the purpose of eavesdropping on private communications or impersonating an otherwise securely authenticated party to a secure communication. As well, cryptographic ciphers may be used as random number generators (e.g. Advanced Encryption Standard used in Counter Mode) or hash functions (e.g. Microsoft Windows's LM Hash used Data Encryption Standard with a constant passphrase to hash passwords).

3.2.2. Weakening Public Use Pseudo-Random Number Generators

Weakening pseudo-random number generators (PRNGs) would help a surveillance agency guess cryptographic keys, nonces, one-time pads, and salts, which are generated using PRNGs. This may be done by placing a bias in the algorithm or entropy source of the PRNG. If any of the above four cryptologic elements are compromised, an attacker or surveillance agency can decrypt private communications, discover passwords, or impersonate parties on a secure communication channel with relative ease.

3.2.3. Weakening Public Use Hash Functions

Weakening hash functions would make authentication of people, communications, and data more difficult. First, hash functions are used to store passwords in a way that cannot be reversed, allowing users to be authenticated without private information being stored in plaintext on the system. Furthermore, cryptographic salts, which are random values generated by hash functions that are padded to passwords prior to hashing, make the assistance of rainbow tables obsolete in attacking passwords. Second, hash functions are used to create message digests

for verifying the integrity of large messages and data in transit over an unsecured channel. Compromising these message digests would allow a surveillance agency to impersonate or tamper with communications or traffic without being discovered.

3.3. COLLABORATING WITH PRIVATE SECTOR TO WEAKEN ANTI-SURVEILLANCE TOOLS

3.3.1. Paying Private Sector Companies to Use Weak Cryptography

Once the public has already obtained the cryptographic ability to prevent eavesdropping by a surveillance state, an attractive covert option is to encourage private sector companies, either by suggestion, compensation, or force, to use weak cryptography. This is possible because many of the users of encryption, including mobile device users, web users, and cashiers, rely on other businesses for their encryption needs.

3.3.2. Key Escrow Services

Key escrow services involve surveillance agencies providing the public with the ability to encrypt provided that a copy of the secret keys are held by the government in escrow. This is an attractive overt option for executing surveillance of the public when the public has obtained to use strong encryption. This is in opposition to the straight-forward approach, which is to either hand the public the ability to encrypt or withhold the techniques from the public entirely. What distinguishes key escrow services is that they allow the government to decrypt communications as necessary, while leaving the public protected from non-governmental actors.

3.4. DEFEATING ANTI-SURVEILLANCE TOOLS

3.4.1. Quantum Computing to Directly Defeat Encryption

Much of the rigor of a given encryption technique depends on the ability to attack the cryptosystem using all possible key combinations, also known as “brute-forcing” the cryptosystem. However, quantum computing can bend the brute-force performance curve and potentially make cracking conventional web encryption feasible in our time. If this ability were to be achieved, it would render cryptosystems and hash functions obsolete, allowing for authentication to be spoofed, man-in-the-middle attacks, eavesdropping, and communications tampering.

3.4.2. De-Anonymizing Anonymizing Services

Tor is a technique for anonymizing Internet traffic that is accessible by users and service providers. Although Internet traffic can be encrypted easily by using any major browser or software, the source and destination of the traffic is in the clear. Analogously, the contents of a postal envelope may be invisible if the envelope is sealed; however, the return and destination addresses are visible in order for the postal service to efficiently transfer the envelope from the sender to the destination. Tor anonymizes the source and destination of Internet traffic. This tool appeals to journalists, illicit traffickers of drugs, weapons, pornography, and money, and all those

who fear heavy surveillance and require anonymity. If a surveillance agency would be able to de-anonymize anonymizing services like Tor, they would be able to eavesdrop on traffic, impersonate parties, or execute man-in-the-middle attacks on groups that are most averse to surveillance.

3.4.3. Withholding Zero-Day Vulnerabilities from Security Professionals

Zero-day vulnerabilities are bugs in computer software that are discovered but have yet to be patched or fixed. Consequently, they are very easy to exploit as they are both known and indefensible. For a surveillance agency attempting to exploit a system, they are invaluable. Surveillance agencies obtain zero-days by their own research, from software vendors directly, or by purchasing them from secretive entities that sell exploits without informing software vendors of the vulnerabilities. In the former case, the idea is that software vendors give very sensitive proprietary information to intelligence agencies in return for assistance from the intelligence agencies.

4. SURVEILLANCE EFFECTS CONSIDERED

4.1. PERFORMANCE OUTPUTS

4.1.1. Systems Penetrated

The first output is if the surveillance technique allowed for penetration of systems that would be inaccessible otherwise. This may involve exploitation of hardware or software, side-channel attacks, social engineering, brute-forcing, or even secretly inserting exploits into systems. This also relates to privacy concerns.

4.1.2. Data Collected

The second performance effect is how much bulk data is collected. This can be done with either the consent, by duress, or by exploitation of a data center. This is the central concern of privacy advocates.

4.1.3. Risk to Intelligence Assets

Does the execution of the operation put intelligence assets at risk, including personnel, sources, and techniques, limiting the ability to conduct further operations? The exposure of these assets can cause damage wider than that of the operation itself.

4.1.4. Cooperation with Other Nations

Last, the revelation of the operation can affect a surveillance agency's ability to cooperate on SIGINT activities with other nations. This is different from diplomatic fallout; if an intelligence alliance is broken, other surveillance operations may suffer.

4.2. ECONOMIC OUTPUTS

4.2.1. Revenues/Losses/Profits

Certain collection techniques can yield direct costs and rewards. For instance, they may lead to the seizure of criminal financial assets. On the other hand, the technique itself will cost money in terms of capital costs, variable costs, and manpower.

4.2.2. Lost Trade to Foreign Competitors

This output is the opportunity cost in terms of lost trade to other nations as a result of surveillance programs. This can be measured by changes in foreign trade in certain sectors before and after the revelations of the existence of these programs and by public statements by government and industry officials.

4.2.3. Torts and Damages Due to Breach of Trust

The next kind of economic output is torts and damages due to breach of trust. As a result of the discovery of surveillance programs, lawsuits may be filed. The legal fees and damages from these cases give an impression of the legal exposure and risk that face the surveillance agency when it uses certain programs.

4.2.4. Trade Secrets Lost

The leaking of trade secrets is also an economic output of the model. As a result of surveillance operations and the withholding of zero-day vulnerabilities from the public, the computer systems of industry entities may be breached, yielding the leaking of trade secrets to domestic or foreign competitors, costing funds. This damage to corporate intellectual property may be estimated by industry reports.

4.2.5. Lost Productivity Due to Exploitation

As a result of the exploitation of computer systems, productivity may diminish. If systems are directly damaged or must be taken offline for patching of vulnerabilities, work cannot get done. This is a direct cost to the industry and to consumers who face risks on their own home systems.

4.3. POLITICAL OUPUTS

4.3.1. Popularity

Popularity polls of the executive and legislative branches of government can also indicate how the popularity of officials has been affected by surveillance operations. Perhaps there is context to these numbers; during conflict, the operations may be considered more popular, but during peacetime, less popular.

4.3.2. Foreign Relations

A major political output from the Snowden leaks has been their effect on diplomatic relations between nations. On the one hand, nations have questioned their allegiances because of revelations of spying between countries. On the other hand, the sharing of intelligence data can enhance diplomatic relations between allies.

4.3.3. Effects on Budget and Headcount of Surveillance Agencies

The effect of surveillance operations on the policies and actions of senior policymakers will reflect on whether the operation was worthwhile. Whether a policymaker decides to continue to fund a surveillance operation would indicate if it was justified. This justification can manifest itself in allocated budget funding and headcount.

4.3.4. Civil Liberties Legislation and Judgments

Civil liberties judgments will also be considered a political output. The opinion of judges can shed light on the contemporary consensus on whether the efficacy of a surveillance operation justifies its cost in terms of individual rights. If this balance is upset, the surveillance operation would be struck down or new restrictions would be imposed. In addition, there is data on the Foreign Intelligence Surveillance Court judgments and how many NSA operations are approved or disapproved.

4.4. TECHNOLOGICAL EFFECTS

4.4.1. Costs Due to Inefficiencies in Standardization Process

As a result of tampering in the standardization process, inefficiencies will yield a loss of product effectiveness because the standards themselves will be of lesser quality. As well, because the industry will not trust certain standards, proprietary inefficiencies will result because products will be less interchangeable, hurting consumers and producers.

4.4.2. Adoption of Open Source Software

The migration from a closed source, proprietary software model to an open source, free software model has received much attention as of late. Open source software allows for lower cost, flexible, and up-to-date solutions, at the expense of less firm support options.[2] According to IT security expert Bruce Schneier, open source is the clear winner: “Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice.”[3] The question, though, is how higher surveillance activity affects the migration towards

[2] "What Are the Advantages and Disadvantages of Open Source Software?," United States Department of Health and Human Services, accessed May 06, 2014, http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/OpenSource/softwareadvantage.html.

[3] Bruce Schneier, "Open Source and Security," *Crypto-Gram Newsletter*, September 15, 1999, accessed May 06, 2014,

open source. On the one hand, it discourages exploits by flushing them out to the public. On the other hand, they allow surveillance agencies to access the source code and secretly implement exploits. The great Apple SSL/TLS "goto fail" bug of 2014,[4] critical GnuTLS bug of 2014,[5] and Heartbleed SSL/TLS bug of 2014[6] all involved open source software.

4.4.3. Industry Incentives to Protect Themselves

As a result of higher surveillance activity, organizations will invest more into protecting their IT systems, meaning higher costs and lost productivity, as well as a higher difficulty to conduct further surveillance, which may be positive or negative depending on the user of the model, e.g. a Civil Liberties Organization vs. an Intelligence Agency.

5. SIMULATIONS AND PREDICTIVE CONCLUSIONS

This section includes four simulations of the model, featuring possible stakeholders, including a Civil Liberties Organization, Foreign Relations Dove, Intelligence Agency, and News Organization. Each simulation includes an analysis for that particular simulation, as well as a cumulative analysis following all of the simulations.

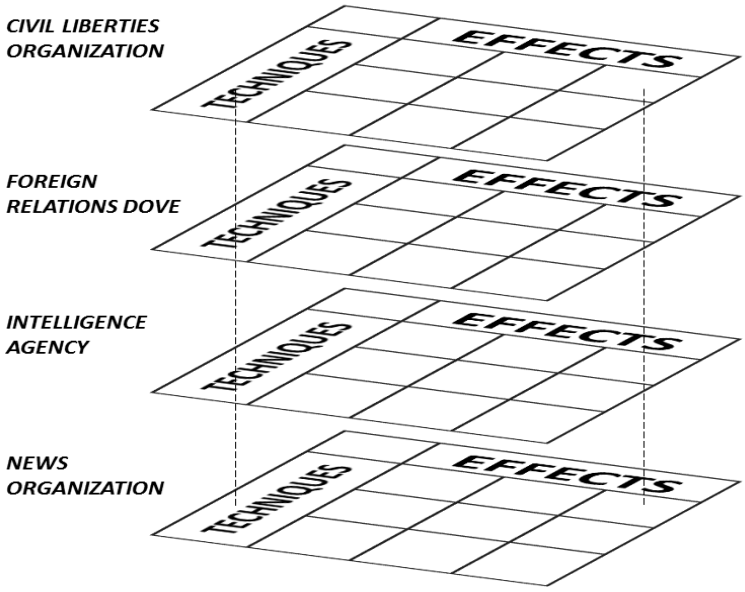


Figure 4 - Various Surveillance Stakeholders Represented by Layered Model Schematics

---

https://www.schneier.com/crypto-gram-9909.html.

[4] Adam Langley, "Apple's SSL/TLS Bug," *ImperialViolet* (blog), February 22, 2014, =, accessed May 06, 2014, https://www.imperialviolet.org/2014/02/22/applebug.html.g

[5] Dan Goodin, "Critical Crypto Bug Leaves Linux, Hundreds of Apps Open to Eavesdropping," *Ars Technica*, March 4, 2014, accessed May 06, 2014, http://arstechnica.com/security/2014/03/critical-crypto-bug-leaves-linux-hundreds-of-apps-open-to-eavesdropping/.

[6] "The Heartbleed Bug," Codenomicon Defensics, April 29, 2014, accessed May 05, 2014, http://heartbleed.com/.

5.1. Civil Liberties Organization

Examples: American Civil Liberties Union, Electronic Frontier Foundation, Electronic Privacy Information Center.

A Civil Liberties Organization prioritizes keeping government transparent and cryptography publicly available and free from interference, but does not place much emphasis on foreign relations and political popularity.

The results are as follows: (Green indicates highest score, red lowest)

Table 1- Model Results for Civil Liberties Organization

Techniques	Score		Effects	Score
Quantum Computing	***2.83***		***Open Source***	***4.32***
Witholding Zero Days	*2.74*		*Risks to Intelligence Assets*	*3.00*
ECC	*2.71*		*Cooperation with Other Nations*	*3.00*
Key Escrow Services	*2.60*		*Trade Secrets Lost*	*3.00*
SHA-3 Modificatinos	*2.21*		*Political Popularity*	*3.00*
Paying RSA to Use Flawed Crypto	*2.21*		*Foreign Relations*	*3.00*
DES Modifications	*2.18*		*Budgets/Headcounts*	*3.00*
Weakening PRNGs	*2.06*		*Torts, Damages, Judgments*	*2.89*
Defeating TOR	***2.00***		*Revenues/Profits/Losses*	*2.81*
Bulk Collection of Google Records	***2.00***		*Lost Trade to Foreign Countries*	*2.81*
Hardware Exploitation	***2.00***		*Incentives to Protect*	*2.41*
			Lost Productivity to Defending	*2.25*
			Systems Penetrated	***1.50***
			Data Collected	***1.50***
			Civil Liberties	***1.50***
			Inefficiencies of Standards	***1.50***

The results of the simulation, which indicated an overall **Cumulative Surveillance Score** of **2.457**, show a slight overall negative impact of the surveillance state in the interests of civil liberties. This is not surprising, since by nature, civil liberties organizations would be averse to surveillance activity in general. The analysis shows that while certain effects obviously contributed greatly to the Cumulative Surveillance Score, e.g. data collection, standards adoption, and civil liberties, there were certain surveillance techniques stood out as well. These included modifications to standards, bulk collection of data, hardware exploitation, defeating Tor.

5.2. Foreign Relations Dove

Examples: Department of State, Ministry of Foreign Affairs, North Atlantic Treaty Organization (NATO), European Union (EU)

The foreign relations dove is keen on maintaining good foreign relations with as many nations as possible, even at the expense of civil liberties and a nation's own security. As well, free trade is emphasized over profits at home. To the foreign relations dove, collaborative operations, free trade, not attacking others, and standards are important. On the other hand, civil liberties are not as important.

The results are as follows:

Table 2 - Model Results for Foreign Relations Hawk

Techniques	Score		Effects	Score
Paying RSA to Use Flawed Crypto	***3.16***		***Lost Trade to Foreign Countries***	***4.27***
Defeating TOR	*3.10*		*Open Source*	*4.05*
Key Escrow Services	*3.00*		*Incentives to Protect*	*3.68*
DES Modifications	*2.96*		*Systems Penetrated*	*3.56*
ECC	*2.90*		*Cooperation with Other Nations*	*3.55*
Weakening PRNGs	*2.89*		*Data Collected*	*3.29*
SHA-3 Modifications	*2.88*		*Lost Productivity to Defending*	*3.24*
Quantum Computing	*2.81*		*Political Popularity*	*3.00*
Withholding Zero Days	*2.71*		*Budgets/Headcounts*	*3.00*
Bulk Collection of Google Records	*2.68*		*Revenues/Profits/Losses*	*3.00*
Hardware Exploitation	***2.18***		*Civil Liberties*	*3.00*
			Foreign Relations	*2.86*
			Risks to Intelligence Assets	*2.56*
			Trade Secrets Lost	*2.55*
			Torts, Damages, Judgments	*2.47*
			Inefficiencies of Standards	***2.11***

The simulation yielded a **Cumulative Surveillance Score** of **2.989**, indicating a slight negative surveillance impact overall, in the interests of foreign relations. Major positive contributions in effects include exposure of sources and techniques, lost trade to foreign countries, promotion of open source, and incentives to protect. The general idea of these aspects is that the adversarial role of some surveillance techniques drives the market to explore techniques of defending against surveillance in a more transparent way. A major negative contribution was how surveillance impacts standards and makes them inefficient, as international organizations don't trust them and find them ineffectual. For instance, due to known tampering with cryptographic standards, achieving the trust of those standards will be very difficult. The most significant positive surveillance techniques were paying RSA to use flawed cryptography and defeating Tor. Although these two techniques are focused on attacking publicly-used cryptography, they would prove to be successful in promoting a decentralized cryptography (as opposed to migrating towards the services of the American corporation, RSA) and forming a better tool than Tor. The most significant negative surveillance technique was hardware exploitation. As is known from the China-US dispute on this issue,[7] this technique tends to sow great international discord.

5.3. Intelligence Agency

Examples: National Security Agency, Government Communications Headquarters, Communications Security Establishment Canada, Director of National Intelligence

[7] David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times* (New York), March 22, 2014, New York ed., International sec., accessed March 23, 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?hp&target=comments#commentsContainer.

Intelligence agencies are focused on fulfilling their mission to ensure the national security of their constituents. They are also concerned with foreign relations if it helps their national security mission, and in the funding of their own agencies. Civil liberties are not a high priority for intelligence agencies and they are indifferent to economic factors. Obviously, they are very concerned about protecting their sources and methods and would prefer to use less overt techniques when possible.

The results are as follows:

Table 3 - Model Results for Intelligence Agency

Techniques	Score		Effects	Score
Defeating TOR	***3.31***		***Systems Penetrated***	***4.23***
Quantum Computing	*3.10*		*Data Collected*	*3.93*
ECC	*3.09*		*Budgets/Headcounts*	*3.41*
Paying RSA to Use Flawed Crypto	*2.99*		*Cooperation with Other Nations*	*3.29*
Key Escrow Services	*2.99*		*Open Source*	*3.20*
SHA-3 Modifications	*2.90*		*Risks to Intelligence Assets*	*3.11*
Withholding Zero Days	*2.71*		*Lost Trade to Foreign Countries*	*3.00*
Bulk Collection of Google Records	*2.68*		*Lost Productivity to Defending*	*3.00*
Weakening PRNGs	*2.63*		*Political Popularity*	*3.00*
DES Modifications	*2.62*		*Revenues/Profits/Losses*	*3.00*
Hardware Exploitation	***2.25***		*Civil Liberties*	*3.00*
			Torts, Damages, Judgments	*3.00*
			Foreign Relations	*2.81*
			Trade Secrets Lost	*2.76*
			Inefficiencies of Standards	*2.70*
			Incentives to Protect	***2.36***

The results of the simulation yield a **Cumulative Surveillance Score** of **2.977**, indicating little overall impact by surveillance agencies. This is significant because it is the intelligence agencies that are conducting the surveillance. Therefore, they ought to be having a larger significant positive impact as they fulfill their missions. There were, however, some strong positive impact effects, including system penetration and data collection, which were particularly strong. The worst performing effects were exposure of sources and techniques and incentives to protect as a result of surveillance activity. For the former, leaks, especially from Snowden, have called into question the ability of SIGINT agencies to be discrete in their activities, jeopardizing their sources and techniques. For the latter, i.e. incentives to protect, the exposure of surveillance activity has caused the public to invest more in defending itself. The best performing techniques are using quantum computing to defeat cryptography and defeating Tor. This is because when effective, these techniques do not destroy public trust, ruin foreign relations, and are the most technologically advanced ways to defeat anti-surveillance measures. However, they are each among the most difficult surveillance techniques, and their effectiveness remains to be seen, especially regarding quantum computing.

5.4. News Organization

Examples: *Associated Press*, *Guardian*, *New York Times*, *Washington Post*.

News organizations value transparency above all else, for both ideological and business reasons. What distinguishes a news organization from a civil liberties organization is that the news organization calls for transparency, while a civil liberties organization also calls for privacy. The news organization does not mind breaches of privacy as long as reporting is not interfered with. Consider that news organizations conduct surveillance of their own kind, i.e. collecting information about other entities, albeit without the threat of law enforcement. Yet, protecting the sources for journalists are important, and that is why many of them use Tor.[8]

The results are as follows:

Table 4 - Model Results for News Organization

Techniques	Score		Effects	Score
ECC	***3.04***		***Open Source***	***3.77***
SHA-3 Modifications	*3.01*		*Risks to Intelligence Assets*	*3.68*
Weakening PRNGs	*3.01*		*Data Collected*	*3.36*
DES Modifications	*2.96*		*Cooperation with Other Nations*	*3.10*
Quantum Computing	*2.91*		*Budgets/Headcounts*	*3.04*
Bulk Collection of Google Records	*2.90*		*Political Popularity*	*3.00*
Key Escrow Services	*2.75*		*Revenues/Profits/Losses*	*3.00*
Withholding Zero Days	*2.75*		*Trade Secrets Lost*	*3.00*
Hardware Exploitation	*2.72*		*Inefficiencies of Standards*	*3.00*
Paying RSA to Use Flawed Crypto	*2.46*		*Torts, Damages, Judgments*	*2.88*
Defeating TOR	***1.71***		*Systems Penetrated*	*2.78*
			Incentives to Protect	*2.70*
			Lost Trade to Foreign Countries	*2.68*
			Lost Productivity to Defending	*2.54*
			Civil Liberties	*2.49*
			Foreign Relations	***2.34***

The simulation yielded a **Cumulative Surveillance Score** of **2.854** indicating a slight negative impact by surveillance agencies. The highest performing effects were that Open Source would be promoted and as far as the interests of news organizations, the risks to intelligence assets would increase, reflecting increased transparency. Poorly performing effects were Foreign Relations and Civil Liberties. The best surveillance techniques for News Organizations were ECC, followed by Weakening PRNGs and SHA-3 Modifications. News Organizations are particularly interested in cryptography, as it helps them protect sources, e.g. Snowden himself, who probably used encrypted email to communicate with journalists.[9] A particularly negative surveillance technique, with a very low score of 1.77, was Defeating Tor. As mentioned earlier in this section, journalists rely on Tor to communicate while reporting within oppressive regimes.

[8] "Who Uses Tor?" The Tor Project, accessed May 07, 2014, https://www.torproject.org/about/torusers.html.en.
[9] Spencer Ackerman, "Lavabit Email Service Abruptly Shut Down Citing Government Interference," *Guardian*, August 09, 2013, accessed May 07, 2014, http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden.

5.5. Commonalities

Based on the three simulations considered in Section 5, some commonalities were discovered between the results of all the simulations. Consider the summary tables below:

Table 5 - Cumulative Results for Techniques and Effects from All Stakeholders

Techniques	Score		Effects	Score
ECC	***2.93***		***Open Source***	***3.84***
Quantum Computing	*2.91*		*Cooperation with Other Nations*	*3.23*
Key Escrow Services	*2.83*		*Lost Trade to Foreign Countries*	*3.19*
SHA-3 Modifications	*2.75*		*Budgets/Headcounts*	*3.11*
Withholding Zero Days	*2.72*		*Risks to Intelligence Assets*	*3.09*
Paying RSA to Use Flawed Crypto	*2.70*		*Data Collected*	*3.02*
DES Modifications	*2.68*		*Systems Penetrated*	*3.02*
Weakening PRNGs	*2.65*		*Political Popularity*	*3.00*
Bulk Collection of Google Records	*2.56*		*Revenues/Profits/Losses*	*2.95*
Defeating TOR	*2.53*		*Trade Secrets Lost*	*2.83*
Hardware Exploitation	***2.29***		*Torts, Damages, Judgments*	*2.81*
			Incentives to Protect	*2.79*
			Lost Productivity to Defending	*2.76*
			Foreign Relations	*2.75*
			Civil Liberties	*2.50*
			Inefficiencies of Standards	***2.33***

Results:

Hardware exploitation seems to have the worst reputation in both the Foreign Relations Dove simulation and the Intelligence Agency simulation. This surveillance technique may be especially onerous because it is both difficult to implement and comes with high risk in the international governmental and commercial arena. In the international governmental arena, Hardware Exploitation has been extremely controversial and hotly contested between the United States and China. On the commercial scene, Hardware Exploitation has caused consumers to lose confidence in US manufacturers, which may cause revenue to flee. The flight of hardware development also makes further Hardware Exploitation itself more difficult.[10]

Defeating Tor was the worst technique for the Civil Liberties Organization and News Organization and best technique for the Intelligence Agency. For civil liberties, Tor is especially important as it is considered an essential tool for anonymizing users in oppressed regimes. For News Organizations, Tor is essential for operating in harsh political climates. As such, the defeat of Tor by intelligence agencies would be a stunning blow to those evading surveillance.

On the other hand, for Intelligence Agencies, defeating Tor would be a resounding success. Tor is used by criminal organizations and dissenters to evade surveillance, and is readily available online.[11] It would be a major victory for intelligence agencies, as well, because it is the only mainstream technique for truly anonymizing Internet traffic.

---

[10] David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway Into Computers," *New York Times*, January 14, 2014, New York ed., International sec., accessed April 29, 2014, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0.

[11] "Download Tor," The Tor Project, accessed May 01, 2014, https://www.Torproject.org/download/download-easy.html.en.

Inefficiencies of Standards is a maximum negative effect for both Foreign Relations Doves and Civil Liberties Organizations. Standards are non-excludable non-rivalrous public goods that lower the barrier to entry and enhance the productivity of all players in the market. Additionally, they may be considered more secure, as they involve the comparative advantage of all players' experts in their standardization. Civil Liberties Organization prefer widely-accepted standards because open governance and the scrubbing of backdoors from anti-surveillance systems is very important to those organizations. For Foreign Relations Doves, standardization bridges international entities and strengthens international commerce and competition.

In all, Table 5 gives an overall picture of all of the techniques and effects compared to each other. The best performing effect by far is the promotion of Open Source practices. This means that the best result of the surveillance phenomenon is that the public will be more transparent about its own practices, perhaps to flush out malicious tampering. The worst performing effects were the Inefficiencies of Standards and Civil Liberties. In other words, the tampering with cryptography by surveillance agencies has dealt a huge blow to the public in terms of no longer trusting agreed-upon standards for cryptography. Accordingly, the very existence of surveillance authority undermines Civil Liberties. The best performing surveillance techniques are Quantum Computing and Elliptic Curve Cryptography. This is because developing Quantum Computing to defeat cryptography does not tamper or eavesdrop on anyone's information directly; it may very well be within the surveillance agency's rights and mission to develop Quantum Computing. Elliptic Curve Cryptography performs well because it is a widely-accepted encryption technique today and malicious tampering has yet to be discovered within its usage (as opposed to PRNGs that implement ECC with tampering). The worst performing surveillance techniques are Hardware Exploitation and Defeating Tor. Hardware Exploitation is onerous because it is very difficult to implement, ruins foreign relations, and sows mistrust. Defeating Tor received low marks primarily because journalists and civil liberties activists rely on it to do their work in difficult environments, and attacking Tor puts them in grave danger.

6. CONCLUSION

6.1. Lessons Learned

Evaluating the impact of a given technique on a given effect will always be fuzzy and categorical. At the beginning of the research process for this study, an effort was made to convert a surveillance effect to a universal impact effect, e.g. converting U.S. Dollars of profit and systems penetrated to the 1-5 scale used in this paper. This proved to be infeasible, both due to the time resources available and the fact that attempting to be precise with this conversion would introduce new controversies and systematic uncertainties into this study. However, as mentioned in Section 1.5, the technique of the study is still strong even if the quantitative results are not significant on their own.

Evaluating each technique-effect pair and determining a fixed impact value is not necessary for this study. At the beginning of the research process, an effort was made to attribute scores for each technique-effect pair to justify each value in the model. In the end, only a partial list of suggestions is provided. This is because evaluating more than 100 technique-effect pairs for each simulation would be infeasible and that the evaluations

need only be subjective. However, there is value in providing subjective values. With more resources, this section may be completed in the future.

Last, the primary lesson learned from this study is that surveillance is complicated, has far-reaching effects, and nevertheless, is employed to a huge extent. An all-or-nothing approach to surveillance is not plausible. As long as national security concerns exist, there will always be a surveillance state to some extent. This study provides not only a glimpse into how surveillance is evaluated, but furthermore, at a process for which its evaluation can be improved.

6.2. Further Study

As indicated in Section 6.1, Lessons Learned, this study does leave more questions to be answered. For instance, justifications for suggested technique-effect evaluations for the model are not explicitly explained. Additionally, Section 5, which contains predictive conclusions and simulations, can be expanded to include other scenarios and more in-depth study. Last, the operation of the model, explained in Section 1.5 and Appendix A, may be improved if it was reviewed by experienced policymakers and other experts.

This study may also benefit and be benefitted by policymakers who would review it overall. These policymakers can include other academic experts, civil liberties advocates, military experts, computer scientists, and politicians. At the very least, they would suggest more techniques, effects, and sources. Towards their benefit, they would find the innovative model provided by this study to be informative for their own work.

Last, this study should be accompanied by a user-friendly interface for setting up and executing the model. This may take the form of a website or mobile app. If the model expands with more inputs, outputs, and dimensions, it may need to evolve from a simple Microsoft Excel model to a more advanced database system with its own report generator.

7. ACKNOWLEDGMENTS

This project was supported by the Centers and Institutes Facilitating Fund of The George Washington University's (GWU) Office of the Vice President for Research. The author thanks Professor Lance Hoffman, Director of GWU's Cyber Security Policy and Research Institute, who supervised this project from its conception as an M.A. project through its finish, for his insight, time, and referrals. CSPRI Research Scientist Allan Friedman provided much necessary constructive criticism and introduced me to many others who provided additional advice and interest. CSPRI Lead Research Scientist Costis Toregas and Coordinator Katelyn Anders provided much necessary support throughout the term of this project in the form of organizational and administrative suggestions. Trey Herr, research fellow, contributed to the content and reviewed drafts. Abigail Shriver and Jeffery Liu provided research and technical support. The author greatly appreciates CSPRI's support and for making this project possible.

APPENDIX: Detailed Mathematical Structure of Model

1.1. Assessment of Individual Technique/Effect Pairs

The model involves comparing a set of 11 techniques (explained in Section 3) to 16 effects (explained in Section 4) to evaluate those techniques. For each technique-effect pair, the user must define two variables:

- ***Likelihood*** that input will occur (scale from 1-5, unlikely to likely)
- ***Impact*** of output, should the input occur (scale from 1-5, negative to positive).

The model then performs the following operation to obtain an ***Expected Impact*** variable for each technique/effect pair:

$$Expected\ Impact = \left(\frac{Likelihood - 1}{4}\right)(Impact - 3) + 3$$

The ***Likelihood*** expression rebalances the ***Likelihood*** variable from 1-5 to 0-1 so it can be applied as a fraction. The ***Impact*** expression rebalances the ***Impact*** variable from 1-5 to -2 to 2, such that a neutral impact is considered 0. The final ***+3*** term in the ***Expected Impact*** equation rebalances the result back to a 1-5 scale, yielding a general impact assessment:

Score	*Meaning*
1	High Negative Impact of a given technique based on a given effect
2	Moderate Negative Impact
3	Little Overall Impact
4	Moderate Positive Impact
5	High Positive Impact

In practice, within the model, these terms are represented as follows, in Figure 5:

	Surveillance Effect 1	
Surveillance Technique A	***Likelihood***	***Impact***
	Expected Impact	

Figure 5 – Basic spreadsheet snippet from model's spreadsheet, detailing an technique-effect pair. Italicized fields are input by the user.

In the table above, **green** indicates a user-selectable value (from 1-5), and **red** indicates a calculated value by the model.

For example, within the actual spreadsheet of the model, the values may be look as follows, in Figure 6:

For each Technique+Effect: Assign Likelihood, Impact, Weight (1-Unlikely/Negative to 5-Likely/Positive		***Performance Data***							
		Systems Penetrated		***Data Collected***		***Risks to Intelligence Assets***		***Cooperation with other Nations***	
		Likelihood	*Impact*	*Likelihood*	*Impact*	*Likelihood*	*Impact*	*Likelihood*	*Impact*
Standards Subversion	DES Modifications	*5.00*	*1.00*	*5.00*	*1.00*	*5.00*	*4.00*	*5.00*	*2.00*
	Expected Impact	**1.00**		**1.00**		**4.00**		**2.00**	
	ECC	*3.00*	*1.00*	*3.00*	*1.00*	*3.00*	*4.00*	*3.00*	*2.00*
	Expected Impact	**2.00**		**2.00**		**3.50**		**2.50**	
	Weakening PRNGS	*5.00*	*1.00*	*5.00*	*1.00*	*5.00*	*4.00*	*5.00*	*2.00*
	Expected Impact	**1.00**		**1.00**		**4.00**		**2.00**	
	SHA-3 Modifications	*4.00*	*1.00*	*4.00*	*1.00*	*4.00*	*4.00*	*4.00*	*2.00*
	Expected Impact	**1.50**		**1.50**		**3.75**		**2.25**	

Figure 6 – Large snippet from model's spreadsheet. The red and green circles next to each value indicate if a value is weak/negative (red) or strong/positive (green).

1.2. Assessment of Overall Techniques and Effects

At the end of each row and column, a raw average is calculated of ***Expected Impact,*** yielding an unweighted sum for each technique or effect:

$$Unweighted\ Score(Input\ or\ Output) = \frac{\sum_{i=1}^{n} Expected\ Impact_i(Input\ or\ Output)}{n}$$

In the model's spreadsheet, that is manifest as the sum of a row or column, as shown in Figure 7:

For each Technique+Effect: Assign Likelihood, Impact, Weight (1-Unlikely/Negative to 5-		***Technological Data***			***Unweighted Score of Technique***	***Standard Deviation***	***Weight of Technique***	***Weighted Score of Technique***
		Inefficiencies of Standards	**Open Source**	**Incentives to Protect**				
Direct Attacks on Systems	Bulk Collection of Google	5.00 1.00	5.00 4.00	5.00 2.00				
	Expected Impact	1.00	4.00	2.00	2.00	0.99	5.00	***2.00***
	Hardware Exploitation	5.00 1.00	5.00 5.00	5.00 1.00				
	Expected Impact	1.00	5.00	1.00	2.00	1.17	5.00	***2.00***
Unweighted Score of Effect		1.50	4.32	2.41				
Standard Deviation		0.55	0.68	0.76				
Weight of Effect (1-5)		5.00	5.00	5.00				
Weighted Score of Effect		***1.50***	***4.32***	***2.41***				

Figure 7 – Snippet from model's spreadsheet indicating the unweighted scores of rows (techniques) and columns (effects). The sums are not true since many of the techniques and effects are omitted from the figure.

Again, the user should consult the impact assessment table to understand the meaning of a score:

Score	***Meaning***
1	High Negative Impact of a particular technique **or** High Negative Impact overall according to an effect.
2	Moderate Negative Impact
3	Little Overall Impact
4	Moderate Positive Impact
5	High Positive Impact

The user then picks a ***weight*** for each technique and effect, on a scale from 1-5 (light to heavy). The final score of each technique and effect is determined as follows:

$$Weighted\ Score(Method\ or\ Metric) = \left(\frac{Weight - 1}{4}\right)(Unweighted\ Average - 3) + 3$$

This ***Weighted Score*** indicates how large of an impact, either positively or negatively, a particular technique or effect will have on the ***Cumulative Surveillance Score.*** The reason for the subtractions and divisions is to rebalance the weight to a 0-1 scale and the unweighted average to a -2 to 2 scale.

Note: If a weight of 1 is assigned to a ***technique*** or ***effect,*** than the effect of those values on the ***Cumulative Surveillance Score*** will always be set to 3 by the model.

1.3. Assessment of Overall Surveillance Strategy

The model allows for an overall assessment to be made of the overall surveillance strategy of a surveillance agency under test. The ***Cumulative Surveillance Score*** is an average of all

of the ***Weighted Scores of Techniques and Effects.*** In this equation, m and n represent the total amount of techniques and effects, respectively.

$$\textbf{\textit{Cumulative Surveillance Score}} = \frac{\frac{\sum_{i=1}^{m} Weighted\ Score\ of\ Method(i)}{m} + \frac{\sum_{j=1}^{n} Weighted\ Score\ of\ Metric(j)}{n}}{2}$$

The meaning of the ***Cumulative Surveillance Score*** is based on the preceding tables as well:

Score	***Meaning***
1	High Negative Impact of a surveillance agency overall
2	Moderate Negative Impact
3	Little Overall Impact
4	Moderate Positive Impact
5	High Positive Impact

As well, for reach technique and effect, a ***Standard Deviation*** is provided to assess if individual elements of each technique or effect deviate greatly from the average or reflect the average very closely.

Caution:

The ***Cumulative Surveillance Score*** is biased towards 3 ("Little Overall Impact") because if a given surveillance agency chooses to employ fewer surveillance techniques or finds that certain surveillance techniques are less impactful, those impact scores of 3 will still be averaged into the ***Cumulative Surveillance Score.*** Mathematically, the ***Cumulative Surveillance Score*** explained in Section 1.3 uses m and n to represent the total amount of techniques and effects, respectively. However, even if some techniques or effects are assigned very low weights, each technique and effect is still counted equally in calculating the ***Cumulative Surveillance Score.*** This makes sense because fewer surveillance techniques will yield a lower surveillance impact overall. However, it will bias the ***Cumulative Surveillance Score*** towards 3 in many cases.