SECURITY THROUGH DEFAULT AND SWIFT DECLASSIFICATION: COOPERATION BETWEEN THE INTELLIGENCE COMMUNITY AND THE CROWD INCREASES ACCOUNTABILITY, TRANSPARENCY, AND RESOURCEFULNESS

Dylan Coyle
Yonsei University

The intelligence community's best resource is the people they are protecting. The lessons learned between from events like the September 11 World Trade Center attack to the 2013 Boston Marathon bombing are that the crowd is wise and creative enough to use the technology and intelligence available to help prevent and recover from manmade and natural crises. Slowing the flow of intelligence to the crowd endangers the lives and freedom of the people which then creates motivation for whistleblowers and leakers to acquire and distribute intelligence themselves. By declassifying most intelligences as a default, and swiftly declassifying old intelligence, the Intelligence Community can maintain critical secrets and preserve privacy while enabling the crowd to analyze and contribute to the body of intelligence to advance international security.

Introduction

The US Intelligence Community has proven to itself that crowds are wise and good at analysis. The public will use the tools they have to analyze information, and today these tools are the same that are used by professionals. Enabled with these tools and accurate information, crowds help solve crimes, save lives, and to recover from as well as prevent crises.

Default declassification introduces a narrow criterion that allows information and intelligence to be hidden as an alternative to current default classification. Swift declassification is investing in Intelligence Community insiders to release as much intelligence as possible as quickly as possible to save resources in the future and allow access to the information now. The public will acquire classified information if it is not given to them, through means such as leaks and whistleblowers. Hiding information also is not effective. The crowd will acquire and use that information to change the world, as seen in the influence of Wikileaks during the Arab Spring. Anticipating default and swift declassification, the parties and individuals affected by the new transparency would have time to change and seek reconciliation for their actions without transparency. Leaks and whistleblowing do not give time for the most diplomatic solutions.

The complications with increased transparency were detailed in David Brin's "Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom" in 1998.[1] He argued that transparency should be reciprocal and intelligence should be shared with the public. Today's debate is not about if intelligence will become available for the public, it is who will do it first. With default and swift declassification, the Intelligence Community can do their job better, using the crowd, to make the world safer.

Theory. The Virtuous Cycle: Accountability, Resourcefulness, and Transparency

For any human organization to function at its best, it needs three things: accountability, resourcefulness, and transparency. An organization evolves based on its feedback derived from how well a system uses resources and how confident this knowledge is, exemplified by the formula (A=R*T). Organizations are not zero-sum systems because resourcefulness and transparency work synergistically to create and improve an accountability system. Like its acronym ART, improving accountability, resourcefulness, and transparency has a steep learning curve initially but experience builds upon itself like learning a new language, instrument, or design program. This paper defines the Intelligence Community as an art and focuses on why default and swift declassification is more resourceful and transparent through better cooperation with "the crowd."

To extend the metaphor, a system focusing on resourcefulness and accountability without transparency is like a RAT, in formula, (R=A/T). The rat is an ingenious animal, which learns and adapts but can ruthlessly pursue its goals.

1 David Brin, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* (Reading, MA: Perseus, 1998).

They are symbolic of unseen destruction, from spreading disease to undermining a house's integrity by chewing through wires and walls. Fittingly, the word for corruption in Spanish is "mordida," or bitten. As one person becomes infected by corruption, they become contagious and can influence others to be corrupt and stall transparency, continuing the voracious cycle. A common fallacy against declassification is that privacy, security, and competitiveness will be lost, assuming Intelligence is a zero-sum game. Instead, crowds and Intelligence Communities that share information and communication tools are significantly more secure, robust, adaptable, and accurate.

An alternative is to accept lower quality service while being aware of the system's flaws. Transparency and accountability without resourcefulness, creates a dinosaur-like system, too big and slow to change, and stuck in TAR (T=A/R). Like the petroleum industry, the true cost includes war, maintaining oppressive regimes, and harm to people's health and their environment.[2] While these costs are known, the cost to change to a sustainable system is higher in the short term. Less-than-optimal short term decisions influence the future as a vulnerable cycle, as "Infrastructure is destiny."[3] The slow and inflexible TAR system creates conditions for the clever rat to win. Information "wants" to be free. Fearing the outcome of sharing intelligence leads to less optimal dissemination because of leaks and whistleblowing. Default and swift declassification maintains security, privacy, and competitiveness more than whistleblowing, and leaks.

Finally, a system with transparency and resourcefulness but without accountability creates a vicious cycle that leads to poverty (TR-A=P). Abhijit Banerjee and Esther Duflo explained how there is a difference in someone who is stuck in a poverty trap and someone who is just poor. The poverty trap is when a person or community have fallen into a vicious cycle, such as losing one's health and livelihood by getting sick from mosquitos, or being crushed under mounting debt on a farm. In a poverty trap, a big push like mosquito bed-nets or free fertilizer for one season can be effective and focused aid. However, if the situation is not an example of such a trap, then any aid is just a redistribution of wealth.[4] Declassification can help discover who is trapped, what the underly-

2 Garth Lenz, "The true cost of oil," Filmed November 2011, TEDxVictoria video, Posted February 2012, http://www.ted.com/talks/garth_lenz_images_of_beauty_and_devastation.html.

3 Robin Chase, "A Conversation with Robin Chase," *Urban Omnibus and The Infrastructurist*, June 2009), http://urbanomnibus.net/2009/06/a-conversation-with-robin-chase.

4 Abhijit Banerjee and Esther Duflo, *Challenges of World Poverty*, (Lecture Notes, Massachusetts Institute of Technology, Spring 2011), http://pooreconomics.com/sites/default/files/14.73_Intro_Lecture2.pdf.

ing causes are, and connect those people and communities with others who can help.

Without a doubt, the Intelligence Community can and must aspire to the highest levels of accountability, resourcefulness, and transparency. The price of secrecy is estimated at over US $10 billion for the American government each year[5] and over US $1.5 trillion globally for the past 20 years.[6] The cost of compromised civil liberties, including privacy and freedom of expression is not included in the equation, nor is the preciousness of life and diversity lost.

Experts are optimistic and show a number of signs that transparency is improving every year. These include constant improvements in the Price Waterhouse Coopers Opacity Index, Transparency International Corruption Perception Index, A.T. Kearney/Foreign Policy Globalization Index, the number of Freedom of Information Acts passed within the US and internationally, and presence of more official Ombudsman in governments.[7] This paper will focus on the improvements in transparency within the Intelligence Community in the US. The room for improvement is significant. Strict procedures for classifying new intelligence and speedy declassification of most archived intelligence would be a significant step towards a more secure and diplomatic world. Transparency does not mean less resourceful, effective, or efficient; a transparent Intelligence Community is better in the long run, offsetting any temporary costs for changing.

Research from the US Intelligence Community

The US Intelligence Community has been researching the benefits of using new technology for sharing information and analyzation, within the IC and with the public. After September 11, 2001, the US Intelligence Community made a concerted effort to share intelligence between agencies, as well as release more information to the public. Defense intelligence analyst Matthew S. Burton wrote "How the Web Can Relieve Our Information Glut and Get Us Talking to Each Other" in 2005. His aspiration was to help analysts connect the dots on security issues after the intelligence failures of 9/11. In 2006, the US Intelligence Community announced Intellipedia, a wiki-based site to share intelligence within the

5 Siobhan Gorman, "The Price of Secrecy: Billions," *Wall Street Journal*, June 2010, blogs.wsj.com/washwire/2010/06/25/the-price-of-secrecy-billions/.

6 David Balaban, "Open Everything – Interview with Robert David Steele Vivas, Part 3," *Privacy PC*, April 2013, http://privacy-pc.com/interviews/open-everything-interview-with-robert-david-steele-vivas-part-3.html.

7 Burkart Holzner and Leslie Holzner, *Transparency in Global Change.* (Pittsburgh, PA: University of Pittsburgh Press, 2006).

IC. Intellipedia helps resolve many of the long ingrained issues within the IC. "Intellipedia embraces the three core principles of social software in enterprise: work at the broadest audience possible; think topically, not organizationally; and replace existing business processes.... This not only helps build institutional memory over time, it provides a foundation upon which future intelligence can be based."[8] Intelligence failures occurred more from unorganized intelligence than from unknown variables. In this manner, the public is already assisting the construction of Intellipedia.

> Interestingly, there have been several incidents when high-level personnel within the intelligence community have requested that some pages on the wiki be removed since they were too sensitive. What is stunning however is that these sites were exact copies of pages on Wikipedia. More than 90% of intelligence information is collated from open sources.[9]

The challenge is to declassify more of the remaining 10 percent of intelligence. Why limit this intelligence to a protected server when it could inform the broader informal intelligence community and public to make more informed choices and contribute to their own security?

Thomas Blanton of the National Security Archive outlined 5 steps to define what should be classified and what shouldn't. 1) Make intelligence unclassified as default; 2) Narrowly define exceptions; 3) Only classify the intelligence according to these exceptions if it can cause identifiable harm to a legitimate cause; 4) This harm to the cause must outweigh any gain from having the information open; and 5) An independent authority should mediate discrepancies.[10] The 1966 International Covenant on Civil and Political Rights, Article 19: Freedom of opinion and expression (to seek, receive, and impart info) defines the narrow range when secrets are appropriate as when the good the transparency will bring is outweighed by the hardship it can cause to the rights and reputation of individuals, national security, public order, and public health/morals.

Judging by the intelligence released by Wikileaks, a significant amount of intelligence does not match these criteria and should immediately be declassified. Only the dangerous and necessarily private information should be secret—

8 Patrick Meier, "Intellipedia for Humanitarian Warning/Response?," *iRevolution* (April 2009), http://irevolution.net/2008/04/09/intellipedia-for-humanitarian-warningresponse/.

9 Ibid.

10 Burkart Holzner and Leslie Holzner, *Transparency in Global Change* (Pittsburgh, PA : University of Pittsburgh Press, 2006).

information that clearly shouldn't be leaked by whistleblowers. This procedure should be complemented with the declassification of intelligence that also falls outside these narrow criteria.

> The cost is minimal compared to the ever-increasing drain on resources created by the growing mountain of classified material that has to be protected — forever! It is a matter of priorities.... Judicious use of retired CIA officers to do declassification reviews could be done at relatively modest cost, leaving serving CIA officers to go about the current business of the Agency.[11]

Declassifying intelligence frees resources while also helping the Intelligence Community to act like a wise crowd and improve analytical output.

NEEDED FOR WISE CROWDS[12]	DESTROYS WISDOM OF CROWDS
Diversity of opinion (even outliers are important)	Homogeneity (lack of diversity)
Independence (opinions aren't determined by peers)	Imitation ("information cascade," lack of diversity)
Decentralization (specialized and local knowledge)	Centralization (distance) Division (silos)
Aggregation (collect and make a collective decision)	Emotionality (peer pressure, herd instinct, collective hysteria)

According to James Surowiecki, a crowd needs four things to act wise: diversity of opinion, independence, decentralization, and aggregation.[13] Opening intelligence promotes the diversity and independence needed for wise crowds. The professional analysts benefit from the added variety and accountability. In 2011, Clint Watts, senior fellow at the Foreign Policy Research Institute, showed the groupthink in the experts. He started a survey about future terrorism issues among experts and a random sample of people. Five days after the start of the survey, Osama bin Laden was killed.

11 Warren F. Kimball, "Openness and the CIA," *Studies in Intelligence*, Winter-Spring 2001, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no5/html/v44i5a08p.htm.

12 James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*, (Anchor, 2005).

13 Ibid.

> The crowd demonstrated the potential to be swayed by popular sentiment or media reporting. For example, the academics in the sample clustered around one answer before Bin Laden's death and then shifted en masse to another answer after his death. This raises important questions about whether to use outside academic experts to fill knowledge gaps in government communities or for assistance with estimating the future course of events.[14]

However, instead of dismissing academics and experts as a whole, the researchers considered research by Philip Tetlock and Isaiah Berlin, who were able to separate the outliers from masses influenced by their peers. Compared to the average sampling, the outliers regularly gave a variety of different answers, were more likely to write their explanation on the survey, and were more accurate. Tetlock noticed that people who were more knowledgeable in many topics (foxes) were better at forecasting than experts in one area (hedgehogs).

Intelligence Advanced Research Projects Activity (IARPA) funded a similar project called Aggregative Contingent Estimation.[15] It is aimed at making better predictions of events through crowdsourcing forecasters. The most accurate members were pooled as the Good Judgment Project and paid US $150 a year for their predictions about various topics. IARPA also found that hedgehogs were useful for thinking of sub-questions on the topics given.[16]

Advanced QUestion Answering for INTelligence (AQUAINT) was another program developed at IARPA. They endeavored to teach computers how to find patterns and make predictions using big data like members of the Good Judgment Project.[17] Machine learning and data mining is most effective in a tight set of parameters: "1) The nature and composition of the underlying data are not changing over time; 2) The data is complete and clean; and 3) You have some idea of what you're looking for."[18] This is not the typical case when looking for "unknown unknowns," or when viewing messy data from something like the Twitter "fire hose" or Prism feed. Accordingly, the Intelligence Community has

14 Clint Watts and John E. Brennan, "Hunting for foxes: Capturing the Potential of Outlier Ideas in the Intelligence Community" *Studies in Intelligence*, Vol. 55, No. 4. 2011, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-4/pdfs-vol.-55-no.-4/Brennan-Reflections%20on%20Outliers-13Jan.pdf.

15 IARPA, 2013, http://forecastingace.com/aces/.

16 Michael Peck, "US intelligence researchers seek public help with forecasting experiment," *C4ISR Journal*, August 2011, http://www.iarpa.gov/Programs/ia/ACE/articles/C4ISR_Journal_article_on_forecasting.pdf.

17 James Bamford, "The New Thought Police: The NSA Wants to Know How You Think—Maybe Even What You Think" *Nova*, 2009. http://www.pbs.org/wgbh/nova/military/nsa-police.html.

18 Palantir, "What we believe," http://www.palantir.com/what-we-believe/.

been pursuing combination of human pattern finding prowess with data surfacing programs.

Chess has been a frontier for comparing geniuses and artificial intelligence. Computers surpassed the best chess-playing humans when Deep Blue defeated chess master Garry Kasparov in 1997. After, competitors began looking at making better computer models to battle each other. In "freestyle chess" there is flexibility in how many humans and computer systems can play in a game. In 2005, a team of amateurs with 4 programs networked together rose to stardom. Their team was named Hydra, after the multi-headed mythological dragon. They beat significantly more sophisticated software as well as world champion chess players by combining human problem solving power with simple but deep analytical tools. The model—commodity hardware networked together and moderately skilled humans—is now used for forecasting real world events as well. Palantir is one software tool used to show multiple data sets to a user at once so they can search for correlations or aberrant subjects within the data set. It runs on Lucene (an open source search engine), Cassandra (an open source data warehousing server), and Hadoop (open source and resource gentle MapReduce framework).

> Palantir's platform is deployed against terrorism, human trafficking, weapons trafficking, drug trafficking, fraud, waste and abuse, child pornography rings and food borne illness. Palantir says its technology is helping public and private sector clients to stop the next Bernie Madoff, genocide in the Sudan, gang violence, Medicare fraud and cyber espionage, and lower the cost of pharmaceutical R&D.[19]

Georgetown University journalism students successful solved the mystery of the murder of Wall Street Journal reporter Daniel Pearl in Pakistan.[20] They successfully matched veins in the hands of the murders in the video to the veins of a torturer in another video.[21] Health care workers could compare Medicare data representing 100 million claims, 1 billion medical procedures, 30 million individual beneficiaries, and 700,000 physicians, and PubMed data representing 22 million biomedical journal articles. They could see possible insurance fraud

19 CNBC, "Disruptor 50: Palantir" May, 2013, http://www.cnbc.com/id/100734736

20 "The Pearl Project released its findings on the kidnapping and murder of Wall Street Journal reporter Daniel Pearl." [Georgetown University, 2010], http://pearlproject.georgetown.edu.

21 "Project Pearl: The Bravest Class in Town," MarieClaire, August 2008, www.marieclaire.com/world-reports/news/terrorism-daniel-pearl-fbi-2.

cases, as well as optimize treatment and funding options.[22] It also reportedly helped in the hunt for Osama bin Laden. Palantir, which is free for non-profits, enables average people with average computer systems to analyze and solve major world issues from home.

Hadoop is a key element of Palantir that distributes data processing over many average computers, forming an inexpensive supercomputer that can handle big data across every range of parameters. The program can also be used on networked computers in remote locations, taking advantage of unused computers in the cloud. It is comparable to the chess program Hydra on a massive scale. Businesses and governments with access to big data are using it to gain insight into consumer and constituent behavior. Hadoop's scale and accessibility has changed the way policy makers and major businesses are making choices.[23] The system would hold "essentially every kind of data there is," said Randy Garrett, who was then director of technology for the NSA's integrated intelligence program. "The object is to do things that were essentially impossible before.[24]

Using big data tools to analyze expected correlations of data is not new. The revolutionary aspect is that any amateur user can casually look at various perspectives of combined data swiftly to find unexpected patterns in Palantir and Hadoop. Analysis and forecasting are then only limited to who has access to the big data. Default declassifying intelligence would make Palantir more powerful for the public; every piece of information is encoded with access level, only the users with the right credentials could see sensitive information. Palantir's secure infrastructure makes it well suited for international security. "Everything a user does in Palantir creates a trail that can be audited. No Russian spy, jealous husband or Edward Snowden can use the tool's abilities without leaving an indelible record of his or her actions."[25]

The focus on accountability with Palantir was intentional, as the founders included Paypal founder Peter Thiel, an avowed libertarian, and Alex Karp, who has a Ph.D in philosophy.

---

22 Ari Gesher. "Palantir at StrataRX 2012: Doing Big Data By Yourself," *Palantir blog*, June 2013. http://www.palantir.com/2013/06/stratarx-2012-doing-big-data-by-yourself.

23 Andrew Leonard, "Netflix, Facebook — and the NSA: They're all in it together" *Salon*, June 2013. www.salon.com/2013/06/14/netflix_facebook_and_the_nsa_theyre_all_in_it_together.

24 Siobhan Gorman, Adam Entous, and Andrew Dowell. "Technology Emboldened the NSA Advances in Computer, Software Paved Way for Government's Data Dragnet" *Wall Street Journal*, June 2013 http://online.wsj.com/article/SB10001424127887323495604578535290627442964.html,

25 Andy Greenberg, "How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut," *Forbes*, August, 2013 http://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/3.

> In a post-9/11 world Thiel wanted to sell those Palantiri-like powers to the growing national security complex: His concept for Palantir was to use the fraud-recognition software designed for PayPal to stop terrorist attacks. But from the beginning the libertarian saw Palantir as an antidote to–not a tool for–privacy violations in a society slipping into a vise of security. "It was a mission-oriented company," says Thiel, who has personally invested $40 million in Palantir and today serves as its chairman. "I defined the problem as needing to reduce terrorism while preserving civil liberties.[26]

This helps clarify why the public has access to the same enterprise technology the CIA is using; the founders believe in checking the vast power the IC has access to with the same tools.

Security data analyst Raffael Marty predicts that by 2020, defense will be impossible, particularly from cyber warfare. "Defense relies on past knowledge. [It's] reactive, always behind. Unknown and new threats won't be detected. Imperfect patterns and rules cause a lot of false positives. Data mining algorithms are built for numerical, not categorical data," and take too many parameters, assumptions, and processing power.[27] His solution is to have systems monitored by people looking at data visually in real time. "Put the human in the loop for understanding, pattern detection, remembering context, fantastic intuition, having predictive capabilities built in."[28] Having live monitoring is more resourceful if relying on open source software, crowd-sourced labor, and pooled best practices. Limiting the amount of data and secrets to be protected efficiently conserves resources for important matters.

Nassim Nicholas Talib takes an encouraging perspective of the worst case scenario in his book Black Swan. He states that history is comprised of many low probability high impact events. Trying to predict the unpredictable is not practical; he suggests building robustness against the knowable outcomes of unpredictable events.[29] An example from "Nate Silver's The Signal and the Noise" is that we know what regions have frequent earthquakes although we can not

26 Andy Greenberg, "How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut," *Forbes*, August, 2013 http://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/2.

27 Raffael Marty, "Cyber Security: How Visual Analytics Unlock Insight," Lecture Notes, KDD Industry Practice Expo, August 2013, http://www.slideshare.net/zrlram/kdd-2013-dm-challenges.

28 Marty, Ibid.

29 Nassim Nicholas Taleb, *The Black Swan*, (Random House, 2007).

predict when they will occur, so we can make buildings resistant and people more ready for when they do happen.[30]

In the book *Antifragile*, Talib dives deeper into the positive outcomes from improbable events. Modern life is filled with fragile structures. Salaried employment has the catastrophic risk of losing one's job. Debt-fueled economies risks implosion. Modern societies push efficiency so hard there isn't enough slack for accidents. Alternatively, we can be antifragile. We can purposely expose ourselves to stress like irregular meal times and violent exercise. We can also invest in things with limited downsides and non-linear unlimited upsides.[31] Maintaining vast quantities of classified information is inherently fragile, as there is "concave" and disastrous risk of being exposed compared to the strength gained from more people being able to utilize the intelligence. Declassification and encouraging people to network to use each other's data is a more robust method of security.

Application: Increased Declassification Aids Security

In the aftermath of the April 15, 2013 Boston marathon bombing people turned to the Internet to participate in the recovery. The effort of local residents was critical to a speedy recovery after the bombing. In the first hour, over two thousand people from disparate communities used Twitter, Google forms, and Google spreadsheets to coordinate distribution of water, food, and shelter.[32] Local Wi-Fi hot spots were opened so people could locate loved ones and share information.

Twitter and Reddit communities attempted to determine the suspects. They "posted pictures taken from the bomb scene and engaged in a large-scale, semi-organized effort to identify the bombers. At one point, users even compiled a spreadsheet of possible suspects, whom they sought to identify." The search lead to one suspect, Sunil Tripathi, and "by morning on the East Coast, Tripathi's name had already been circulated in the press in India and Britain." The conjecture was wrong, but it contributed to the FBI releasing the suspected bombers pictures and videos April 18.[33] Boston Police Commissioner Edward Davis said the release "was a turning point in the investigation, no doubt about

30 Nate Silver, *The Signal and the Noise*, (Penguin Press, 2012).

31 Nassim Nicholas Taleb, *Antifragile*, (Random House, 2012).

32 Patrick Meier, "Self-Organized Crisis Response to #BostonMarathon Attack," *iRevolution*, April 2013, http://irevolution.net/2013/04/16/bostonmarathon-attack.

33 Gerry Shih, "Boston Marathon bombings: How Twitter and Reddit got it wrong," Independent, April 2013, http://www.independent.co.uk/news/world/americas/boston-marathon-bombings-how-twitter-and-reddit-got-it-wrong-8581167.html.

it."[34] The suspects, Tamerlan and Dzhokhar Tsarnaev, were located while fleeing Boston by tracing the phone of a hostage who escaped from a stolen car. Dzhokhar was arrested and Tamerlan was killed during the pursuit.

Patrick Meier, a blogger and advisory board member for the Crisis Map web service Ushahidi described the informal network of helpers as "the crowd." Empowering the people within the crisis with timely access to intelligence can mitigate the limited service and focus of professional help immediately following a crisis. In this case, the crowd created an ad hoc marketplace to redistribute goods and care.

> Getting the information that comes from the crowd and feeding it back. They probably need that information more than the first responders, because who are the real first responders? The disaster affected population themselves. The crowd will always be there. By definition, the crowd is always there and the crowd is many.[35]

Secrets, which can delay the effectiveness of crowd actions, can cost lives. When provided with information that it requires, the crowd is capable of resolving many problems. The emergent nature of crowd feeding helps non-professionals to become their own Intelligence Community.

An example of professional directed crowd feeding was the application called Dagens Nyhete started by Doctors at Swedish hospital Sodersjukhuset. Normal people are trained to help victims of cardiac arrest. When someone is having a heart attack, the closest volunteer is sent a text message with the location to help before professionals can arrive. Survival rate rose from 3 percent before the application to 10.9 now.[36] The IC can share their experiences with the new home analysts in the same way the Swedish doctors trained volunteers to help locally. "Managers must trust their officers to share directly with each other and with the policy community. A manager's role will become less command and control and more teacher of tradecraft and communicator of purpose and objectives."[37] Surely the experts in the IC will have new perspectives and

34 Milton J. Valencia, "Boston Police Commissioner Edward Davis says releasing photos was "turning point" in Boston Marathon bomb probe," *Boston Globe*, http://boston.com/2013/04/20/boston-police-commissioner-edward-davis-says-releasing-photos-was-turning-point-boston-marathon-bomb-probe/sojcZNcTCGah8UYBnRuk9O/story.html#sthash.i7Egqr8p.dpuf.

35 Patrick Meier, "Collaborative Crisis Mapping," Presentation at the Emergency Social Data Summit organized by the Red Cross in Washington DC, August 2010, http://youtu.be/4ANZd6v9qIc.

36 Steve Kelman, "A Public/Private Partnership that is Saving Lives," *The Lecture*, October 2013, http://fcw.com/blogs/lectern/2013/10/stockholm-public-private.aspx.

37 D. Calvin Andrus, "Toward a Complex Adaptive Intelligence Community" Studies in Intelligence, vol

insight to share as well, which can only strengthen international security if the public can learn from them. 60 percent of the CIA is already contractors,[38] so a move to embrace the informal Intelligence community is the next step of distributing analytical labor to more diverse and local talents.

Opening national security is necessary in an interconnected world. The Boston marathon bombing demonstrated the international nature of today's security environment. The Tsarnaev were born in the USSR and Kyrgyzstan. Their reported motives were connected to US foreign policy and the Iraq War and War in Afghanistan. The Russian Federation informed the US of their danger 18 months before the attack.[39] The one of the three spectators killed was a student from China, and the hostage who led to the arrest was also from China. Security experts are distributed across the world, and connecting them with local experts is key to preventing and resolving future crises.

> What distinguishes today's tests and makes the traditional intelligence paradigm less effective is the transnational and global character of many trends.... The compression of time and space and the easy movement of people, weapons, toxins, drugs, knowledge and ideas have transformed the way threats emerge and challenge the way intelligence must operate... planned and launched from many different countries, making the individual actions of any single government or intelligence service ineffective in detecting, deterring or preventing those attacks... many of these the international community's "blind spots," which our current analytical lenses are not to make sense of....[40]

Future extremists must consider that the crowd is an active participant in its own security. Even for lone wolf terrorists like the Tsarnaev, photos incidentally including them can lead to identification and alert citizens can find them hiding in boats behind their houses. In contrast to the Big Brother top-down surveillance

---

49, no 3, 2004, https://cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Wik_and_%20Blog_7.htm.

38 Jesse Finfrock and James Bamford, "Q&A: James Bamford author of The Puzzle Palace, on the CIA's brain drain under Bush," *Mother Jones*, October 2008. http://www.motherjones.com/politics/2008/09/qa-james-bamford.

39 Eileen Sullivan and Julie Pace, "Zubeidat Tsarnaeva, Bombing Suspect's Mom, Also on Terror List," *Huffington Post*, (Retrieved May 1, 2013), April 26, 2013.

40 Roger Z. George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm" CSI Studies, vol 51, no 3, September 2007, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/building-a-global-intelligence-paradigm.html.

society, a surveillance network of the crowd, especially when working with the professional Intelligence Community, is more wise, local, and effective.

The outreach of professional communities to recruit amateurs for analysis is apparent in the increase in the number and complexity of crowdsourcing websites. Liza Alert is a Russian website for finding lost children with 1300 members, 50-70 are active weekly. There are sites for analyzing and classifying photographs, such as satellite data on river-like deltas on Mars on cerberusgame.com or Australian wildfires with Tomnod.com. Users have access to 225 cameras in Tanzania to see and report how species interact with each other on Snapshot Serengeti. Ancient texts and dolphin's sounds are being translated. Users analyze folding dynamics of proteins with FoldIt and RNA with EteRNA, which can then be used to identify disease and create medicine. Computers watch how humans solve the problem to create better algorithms to look at data. On EyeWire, users map the neural pathways of retinas. According to Linus's Law, named after the founder of Linux, "Given enough eyeballs, all bugs are shallow."[41] Author Clay Shirky estimated the educated population of the world has over 1 trillion hours a year of unutilized time, which can be used for complex, crowd-based collaborations.[42] He argues that creating infrastructure that enables collaboration is the best way to capture that lost energy. For the Intelligence community, that requires sharing information, and also sharing the responsibility of analysis.

The Alternative. Leaks and Whistleblowers

If the Intelligence Community doesn't provide transparency though broad, timely, and default declassification, then individuals will feel morally compelled to correct the power asymmetry and become whistleblowers or create information leaks. Transparency is here to protect privacy of the powerless against the powerful. It is critical in any liberal system. The number of leaks and whistleblowers is thus increasing, as there is more need for transparency and accountability to balance the new technology of the Intelligence Community.

It should be understood that transparency does not mean the end of secrets and privacy. In fact, it is through the artful use of transparency that one's power is shown but also tempered and hubris is avoided. Julian Assange sees transparency as a tool for balance, and doesn't expect any person to give up their rights.

41 Eric S. Raymond, *The Cathedral and the Bazaar*, (O'Reilly Media, 1999), p. 30.

42 Clay Shirky, "How cognitive surplus will change the world," *Ted@Cannes*, Filmed June 2010, Posted June 2010, http://www.ted.com/talks/clay_shirky_how_cognitive_surplus_will_change_the_world.html.

> Transparency should be proportional to the power that one has. The more power one has, the greater the dangers generated by that power, and the more need for transparency. Conversely, the weaker one is, the more danger there is in being transparent." In other words, if information is power, then what the transparency movement is trying to do is correct an asymmetric power relationship.[43]

Developments in the defense industry and Intelligence Community make the choices clear: governments can choose declassification, or accountability will be attained through the threat and exercise of less optimal releases of intelligence through journalism, whistleblowing, and leaks. If the organization, government or Intelligence Community is not voluntarily transparent, individuals are conflicted morally and become civilly disobedient to correct the perceived imbalance.

When confronted with what he perceived as injustice, Edward Snowden revealed the US PRISM intelligence program was collecting unprecedented information on international users of US based websites. As declassification was not a valid recourse, he became a whistleblower.

> Snowden...tried to act as principled and professional in his whistleblowing as he could. What he did instead was give up his life of career stability and economic prosperity, living with his long-time girlfriend in Hawaii, in order to inform his fellow citizens ... by very carefully selecting which documents he thought should be disclosed and concealed, then gave them to a newspaper with a team of editors and journalists and repeatedly insisted that journalistic judgments be exercised about which of those documents should be published in the public interest and which should be withheld. That's what every single whistleblower and source for investigative journalism, in every case, does—by definition.[44]

This is complicating relations between the US and its allies and trading partners. If the US anticipated the declassification of this knowledge, they could have made a formal press release about how increasing international security

43 David Le Baily and Julian Assange, "Julian Assange: 'I have no choice. Publish or Perish," trans. Mark K. Jensen, *Paris Match*, December 2010, http://wlcentral.org/node/876.

44 Glenn Greenwald, "On the Espionage Act charges against Edward Snowden: Who is actually bringing 'injury to America': those who are secretly building a massive surveillance system or those who inform citizens that it's being done?" *Guardian*, June 2013, http://www.guardian.co.uk/commentisfree/2013/jun/22/snowden-espionage-charges.

is a priority shared with their allies, and could have worked together to find an acceptable way to share information. As the countries being monitored had records of potential threats within their countries, cross-declassification would ameliorate the same situations better than PRISM. For example, the Russian government informed the US government about the threat of Tamerlan Tsarnaev but the Boston marathon bombings were not prevented. Alternatively, if the public, especially the Boston law enforcement agencies, knew what threats to be aware of, the tragedy may have been stopped early. Further, if Tamerlan Tsarnaev knew that his participation with extremists contributed to his difficulty gaining American citizenship and better employment, he could have made better choices than violence.

On August 21, 2013, Private Manning pleaded guilty and was charged for releasing classified materials to WikiLeaks. Manning did not know how to clean the material himself, nor could he have cleaned the volume alone. The Collateral Murder video was carefully prepared for the media by Wikileaks to represent the embarrassing, illegal, and unethical actions taking place in Iraq by the US military. However, the subsequent Cablegate leak did expose a large number of uncritical documents. According to the ideals of Blanton, these never needed to be classified initially. Contrast with the opinion of Bowman H. Miller, the leaks were belligerent and it was wrong to give them to an Wikileaks instead of journalists because it had a shallow institutional history and little stake in releasing all the files they did.

> Bona fide journalists operate cognizant of an ethical code which, despite their calling to hold government to account, helps to govern their actions and underline their responsibility in dealing with national security issues and information; secondly, those journalists write for a public, large or small, and have a purpose and are selective in their reporting. On the other hand, WikiLeaks' actions have no stated purpose beyond disclosing, without restraint, what it illicitly has received from unnamed sources. Contrary to some claims, the leaker of the vast amounts of Department of State and other reporting was not and is not a whistle-blower. That name only deserves to be used for those revealing embarrassing, illegal, unethical, or negligent behavior by those enjoying the public's trust and confidence. The WikiLeaks leaker defies this definition.[45]

45 Bowman H. Miller, "The Death of Secrecy: Need to Know...with Whom to Share," Studies in Intelligence, Vol 55, No 3, 2011, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-3/the-death-of-secrecy-need-to know...with-whom-to-share.html.

Manning stated the motivation to release the files was to stimulate a public discussion about open diplomacy. Reuters tried to attain the video in 2007 through the Freedom of Information act unsuccessfully, so Manning was compelled to take the files and share them with Wikileaks secretly. Declassification and following the Freedom of Information act could have avoided the shock from the sudden revelations following the Wikileaks cable gate leaks assisted by Private Manning.

> By exposing hidden secrets, double standards, and hypocrisy by Arab leaders they provided new perspectives on Arab politics as well as confirming widespread suspicions, and thus put angry publics in direct confrontation with autocratic governments. Wikileaks offered critical information, contributed to the mass "mediatization" of events both local and internationally, and helped formulate and clarify the critique of the existing political situation and democratic alternatives.[46]

The truth has enormous power, and the holders of the truth have the responsibility to see that it is available to the public for making informed choices, but also that the public has informed in an honest manner to maintain respect and civility through change. For example, if the leaders of the Middle East and North African countries were aware of impending declassification, a discourse with the public could have been started earlier to avoid the embarrassment and violence when other people tell your secrets first. Declassification forces leaders to be diplomatic and mature. On the same point, leaders throughout the international community must anticipate and should participate in declassification, as a leak in one country leads to riots on the other side of the planet.

Default and swift declassification is the best way to help the public make informed choices and provide for their own security. If those benefiting from the lack of transparency must wait until leaks and whistleblowing reveal them, many continue because of a bias to ignore high-risk low probability events and to discount the future. If declassification is chosen, then the beneficiaries must confront their choices. Given today's complex legal system, privacy is one of the only protections for many people committing crimes they see as innocent and victimless. Declassification will reveal how much our laws must mature with the times to create a safer world. For liberal societies, the rule of law is

46 Ibrahim Saleh "Wikileaks and the Arab Spring: The Twists and Turns of Media, Culture and Power." *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society* [2013], 245-253.

critical, but so is the evolution of law through the comfort of privacy and loopholes of religious freedom that provide space to participate in breaking laws and proving they are not needed. Leaks and whistleblowing, though noble in cause, are inferior to the public demanding declassification. It is in the public's interest to protect their privacy with transparency created ethically and with time to allow those endangered by it to come clean first, seek amnesty and show that they will act better in a different future, or highlight why the laws need to be updated. We must amend the adage "You have nothing to fear if you've done nothing wrong," with "but something must change if the law and society don't correspond."

Assange suggests another possible solution: to start encrypting information more. But default encryption is an extremely fragile cycle to continue to encrypt and hide more information that can lead to the keys to the other encryption. Even Osama bin Laden could not completely remove himself from the grid of society.

> Biometric data gathering, facial recognition technology, domestic drone surveillance, and the strategic intersection of all private communication: these are the four horsemen of Assange's apocalypse. ... Now even a country like Libya can afford systems like Eagle, a product sold by the French firm Amesys and used by the Gaddafi regime for mass interception of communication. Even poor countries are setting up surveillance systems: as Muller-Maguhn claims, African countries are getting entire spy network infrastructure as a gift from the Chinese, who expect to be paid back "in data, the new currency."[47]

Declassification will help protect and keep citizens aware of invasions of privacy from others. The future of intelligence and the wise crowd could be further distributed with technologies that bypass central authorities. The wireless mesh technology can link mobile devices directly together to share data. Instead of needing to contact a centrally connected cell tower, each phone or wireless router acts as an access point to each other, allowing users to bounce signals off each other to communicate with users across the continent, or to safe access points in other countries or satellites in orbit. This can have significant impact in countries with oppressive governments as power slips away. The mesh could be activated with hardware already installed in current mobile devices with a

47 Adam Morris, "Julian Assange: The Internet threatens civilization." *Salon*, May 2013, http://www.salon.com/2013/04/30/tk_5_partner_15.

software update. More than 70 organizations have made wireless mesh methods, and progress may be seen after choosing a standard such as IEEE 802.11s: Standard for WLAN Mesh Networking.

Governments are now struggling with services like Weibo and Twitter, but true meshed wireless will possibly be the key for the crowd to negotiate for more rights and privileges, creating the Dictator's Dilemma balancing "information communication technology for economic development with their need to control the democratizing influences of this technology."[48] Patrick Meier wrote about how the Chinese government was already trying to physically block citizens from helping each other after the Lushan earthquake in April 2013, when they could have used the volunteers to help recovery.[49] Increased communication and analytical ability through modern technology is inevitable. Declassifying first can lessen the amount of leaks and whistleblowers. It is in the best interest of the International Intelligence Community, to treat the crowd with respect, train them in tradecraft and ways to help each other, and focus on mutual goals of a more peaceful and just global community.

Conclusion

The role of the Intelligence Community as the keeper of secrets and pinnacle of wisdom is being challenged by their own research. The goal of internal peace and security is best pursued through cooperation and honesty. The recent increases in technology have given governments broad and extreme powers, which the public has fought against with leaks and whistleblowing. Crowds help with security because they are wise and local. Publically available tools like Palatir and Hadoop, and intelligence through technology like spreadsheets, Twitter, and wireless meshes also increase the power of the public, amplifying any mistakes they make. Default and swift declassification combines the best of tradecraft, technology, and the virtues of crowdsourcing. Mistakes are minimized, and the service to peace and security are maximized. **Y**

48 Rachel Naomi Fredman, "The Dictator's Dilemma and the Politics of Telecommunications in Cuba: A Case Study" April 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2043679.

49 Patrick Meier, "How Crowdsourced Disaster Response in China Threatens the Government," *iRevolution*, May 2013, http://irevolution.net/2013/05/21/crowdsource-response-china-quake.