The Opportunities and Limits of Societal Verification

Kelsey L. Hartigan and Corey Hinderstein
Nuclear Threat Initiative

Institute of Nuclear Materials Management
Palm Desert, CA
July 2013

The uptick of interest in information and communication technologies (ICT) continues to generate new thinking in the arms control and nonproliferation sectors. Ripe for further study, public technical means (PTM), as some leading experts are now calling it, have the potential to supplement traditional verification tools and mechanisms, and bolster international confidence in future bilateral and multilateral agreements. As interest in the ICT domain expands, however, fundamental questions related to the reliability and legality of these tools and sources remain. As part of its Verification Pilot Project, the Nuclear Threat Initiative launched its Societal Verification Working Group nearly two years ago in order to examine the role heightened public awareness and vigilance may play in future verification and monitoring regimes. This paper builds on NTI's 2012 INMM submission and the work of NTI's Societal Verification Working Group, detailing new case studies which retroactively track the social media footprint of past incidents, and further analyzes key questions surrounding societal verification tools and processes. We explore mobilization tactics and challenges, areas of overlap and divergence with all source intelligence gathering as well as privacy and legal issues that must be addressed if these tools are to make meaningful contributions to the arms control arena.

Keywords: Societal Verification, Crowdsourcing, Information and Communication Technology

Information and communication technologies have reshaped the ways states, corporations and private citizens share, collect and analyze information. The Internet serves as the bedrock of this transformation, connecting more people and devices than ever before. A recent Council on Foreign Relations task force on Internet governance estimates that by the end of this decade, some six billion people will be online, and as many as 31 billion devices could be connected to the Internet.[1]

Armed with small and relatively inexpensive chips and sensors, the data generated by these devices are being leveraged in new and innovative ways. This “datafication” of society, combined with novel tools and technologies that sort, analyze and even predict, have powerful implications for how states and publics might address the most pressing international security challenges of the 21st century. [2]

[1] CFR Task Force, Defending an Open, Global, Secure, and Resilient Internet, June 2013, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836

[2] Cukier K and Mayer-Schoenberger V; *The Rise of Big Data; Foreign Affairs; May/June 2013*; *http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data?page=show*

OPPORTUNITIES AND POTENTIAL ARMS CONTROL CONTRIBUTIONS

Despite some lingering skepticism, the majority of informed audiences now accept the potential for new types of open source information and tools to supplement traditional arms control verification techniques. The successful introduction of these tools in other sectors – including emergency response, humanitarian relief, disease control and commercial marketing – has demonstrated the value of big data and new and emergent technologies.

The sheer quantity of information available is unprecedented. Analysts can determine the location, temporal characteristics, sentiment and connections of people who choose to publicly share their observations, opinions and photos online. Experts inside and outside of government have access to high volumes of data and sophisticated analytical tools that can collect, fuse and visualize disparate data streams. Some experts are also exploring whether the public can be actively recruited to share certain types of information or invest in personal technologies such as a smartphone equipped with specific sensors. As the field continues to develop and states consider new methods for leveraging these tools and sources of data, it is important to realize that the detection goals, the type of collection method or tool, and the entity utilizing it all influence the value of the information and the degree to which it might contribute to a future arms control regime.

For the past year and a half, NTI's Verification Pilot Project has been examining the opportunities and challenges that accompany a greater public role in verification. While the group is exploring the utility of social media platforms like Twitter and Facebook, the focus extends beyond this to include data gathered through other non-traditional, commercial sources and analysis from nongovernmental organizations, independent scientists and other nonstate actors. The group is working to define a framework for how states might integrate various societal contributions within existing and future verification regimes, and has identified a range of topics for further study.

When the project began, the central challenge appeared to be one of data management – how is the information captured and sorted, and what tools are necessary to overcome language barriers and validate the authenticity of the information. It is now clear, however, that the primary challenges are not necessarily technical, but operational and political. Advancements in software and data analytics continue at breakneck speeds. The challenge comes not in developing new technologies, but in creating a legal and political framework under which the information can be collected, organized and applied. In some cases, open source information derived from societally generated sources is already included in national all source intelligence gathering and analysis. This is in its early stages, however, and this information is not yet integrated into treaty compliance monitoring and verification.

The ability to craft an information architecture that takes advantage of the amount of information that is now available and organizes data in a coherent, accessible manner will largely determine the extent to which new forms of commercial and open source information might be successfully collected and integrated with future arms control verification regimes. How this information is communicated to the public will be equally important. In the wake of the discussion sparked by Edward Snowden, for example, the debate over privacy, security and the role of government has intensified as citizens become increasingly aware of their online footprint, and how their personal data is being used. While data mining is hardly a new phenomena – commercial entities such as Google have long thrived off of consumer data – governments have not effectively communicated what type of information might be collected, and for what purpose. There are serious challenges to consider, but the opportunities are too great to ignore.

Detection Goals

Pinpointing the detection tasks is a crucial first step, and can include a range of objectives. While the parameters of future agreements will dictate what tasks are the most relevant, in general, societal verification can be used to define patterns, identify shifts or outliers, fill in blind spots or detect signals.[3] In the arms control context, this might indicate:

- activities of key technical experts
- acquisition or attempted acquisition of specialized equipment and materials
- movements of delivery vehicles
- preparations for a nuclear test or missile launch
- a nuclear test
- clandestine nuclear activities such as fissile material production or warhead manufacturing

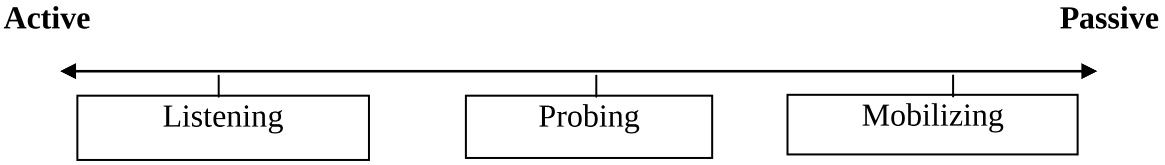
In some rare cases, societal data and devices might be used to directly identify treaty violations. In most instances, these tools are likely to convey information that is only indicative of potential violations or misuse. For example, data gleaned from open source information might provide details on daily routines such as when a facility operates or employees report to work, flag sudden upticks of activity at certain military installations or facilities, or reveal connections or sudden drops in activity among scientists or engineers with specialized training and expertise. None of these are proscribed activities, but such signals could provide additional context or insight into a treaty partner's behavior when integrated with other data streams.

Types and Methods

Detection goals can influence what tools or methods might be used to collect or analyze societal information. There are a range of tools and methods available and the attempt here is not to catalogue or list every tool or technology that could be used in a societal verification regime, but rather to better understand what characteristics influence the value and effectiveness of the various types of societal verification.

[3] Hinderstein C and Hartigan K; *Societal Verification: Leveraging the Information Revolution for Arms Control Verification*; INMM Annual Conference, July 2012.

The Societal Verification Continuum



On one end of the spectrum is passive data collection, or "listening." This can be used to harness content from social networking sites, blogs, microblogs and photo sharing sites.[4] On the other end of the spectrum, active forms of societal verification rely on public involvement, or "mobilization." Rather than simply collecting data that already exists, mobilization requires the tasking of specific actions to individuals or groups who are otherwise generating unspecific information. Crowdsourcing, ubiquitous sensing, and games or challenges can be used to mobilize publics. Many societal verification tools fall somewhere in between, or include elements of both passive and active sensing. Probing, posing a basic question or challenge, but refraining from further engagement, is one such example.

Users

The user determines how the information is utilized. For the purposes of arms control verification, the end-user is the government. Governments party to certain treaties and agreements are responsible for making the final determination as to whether the other parties are complying with their treaty obligations. The information that governments use to make this determination, however, can come from various channels. This is where societal verification is likely to make the most meaningful contribution. Governments, as well as commercial and private entities, can utilize open source information and tools to gain additional insight into a state's nuclear activities. Thus, while there is ultimately one consumer, there are multiple suppliers of raw data and analysis: intelligence analysts, commercial entities, independent experts and the public at large. Whether and how to connect these suppliers will be an important challenge to consider going forward since such analysis currently takes place in separate silos.

CHALLENGES AND LIMITATIONS

Data Management

In order to operationalize the societal verification concept, it will be essential to develop a framework for collecting information and organizing data in a consistent, user friendly format so that the information can be easily analyzed and disseminated. While such a structure does not yet exist for arms control treaty verification purposes, advancements in integrated information management systems in other sectors provide a good model for how such systems might be developed and implemented. For example, experts at Sandia National Laboratories have identified several open source software systems and technologies (such as Zotero, WordPress,

[4] See for example, Whattams K and Gastelum Z, *State-of-the-Art of Social Media Analytics Research;* PNNL; January 2013; http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-22171.pdf

Drupal, etc) that analysts might use to collect, structure, analyze and disseminate geospatial information for safeguards.[5] Innovations in cloud computing have also alleviated data storage and retrieval issues, and while the timely sorting and analysis of massive quantities of information remains a central challenge, this is as much of a personnel and resource challenge as anything.

These data management challenges will require continued research and development, but there is room for optimism as the primary hurdles to implementation are not necessarily technical in nature. Growth in innovative software programs and big data expertise have far outpaced the requisite policy and legal frameworks, making the central challenge one of how to integrate societal verification information with existing data streams for arms control verification.

Integration

Within the IC, interest in open source information has significantly expanded in recent years. The 9/11Commission and WMD Commissions both emphasized the importance of open source information. In fact, the WMD Commission specifically recommended: "The DNI should create an Open Source Directorate in the CIA to use the Internet and modern information processing tools to greatly enhance the availability of open source information to analysts, collectors, and users of intelligence."[6]

Past press reports and speeches indicate that the IC has been collecting open source information from new media for several years. In fact, as early as 2007, the director of the Open Source Center, which was launched in 2005 in response to the WMD Commission's recommendation, was highlighting the value of what he called "Citizens Media:"

> A couple years back we identified Iranian blogs as a phenomenon worthy of more attention, about six months ahead of anybody else. We're now looking at YouTube, which carries some unique and honest-to-goodness intelligence. There are methodologies involved. We're looking at chat rooms and things that didn't even exist five years ago, and trying to stay ahead. We have groups looking at what they call "Citizens Media," people taking pictures with their cell phones and posting them on the Internet. Then there's Social Media, phenomena like My Space and blogs. And then there's what we call Mobile Media. In Africa, they skipped a whole generation of communications. People carry photo albums on their cell phones and share the photos. Their cell phones are a big part of their lives. All these phenomena affect not only the context of Open Source, but how people interact.[7]

While the technologies have already evolved significantly over the last several years, it is clear that open source information derived from societally generated sources is already included to some extent in national all source intelligence gathering and analysis. This is in its early stages,

[5] McDaniel, Bleakly and Horak, "Exploiting the Geospatial Dimension of Data in Support of IAEA Safeguards," ESARDA Bulletin, No. 47, June 2012.

[6] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 31 March 2005, page 377.

[7] Doug Naquin, Central Intelligence Retirees' Association Luncheon Remarks, 3 October 2007

however, and this addition to all source intelligence is not practically integrated into treaty compliance monitoring and verification determinations. Given the vast amount of information available, this is likely the result of a basic resource constraint. In the United States, for example, arms control verification is not a priority for open source intelligence analysts who tend to focus on terrorism and areas of unrest.

Public-private partnerships could help leverage the tools and information now available in the open domain, while facilitating more transparency and public trust in how their information is being used. In fact, experts in academia and the private sector already operate open source, new media centers. For example, The Center for Geospatial Intelligence (CGEOINT) at George Mason University focuses on "research that relates to geospatial and spatiotemporal information extraction, analysis, and visualization. This includes image and video processing and analysis for information extraction, harvesting geospatial information from social media feeds, geosensor networks, spatial and spatiotemporal databases, spatiotemporal modeling and analysis, and complex visualization solutions."[8] The MITRE Corporation has also developed what it calls its Social Radar. As MITRE analysts explain: "Such a system would support strategic- to operational-level situation awareness, alerting, course of action analysis, and measures of effectiveness for each action undertaken. Success of a social radar depends on continuous access to global data on perceptions, attitudes, opinions, sentiments, and behaviors. Much of the most timely and valuable data will be found in social media applications such as Facebook, Twitter, Flickr, YouTube, and various blogs."[9]

Opportunities to pair such efforts with the Open Source Center, which would serve as the main vehicle for integration with other IC data streams, need to be further researched and should be seriously considered going forward. Additionally, the specific questions and queries suitable for societal verification efforts need to be better defined.

Public and Private Contributions

In addition to exploring public-private partnerships, more thought needs to be given to how commercial and nongovernmental entities, independent scientists and other nonstate actors might feed into future verification efforts. It is important to distinguish between what the general public might be expected to contribute, and what a network of outside analysts might bring to the table.

Public familiarity with treaties, and treaty limited items is limited. Verification tasks aimed at mobilizing the public present several challenges, and would require a significant investment in public education. For example, the runner-ups of a recent State Department challenge proposed creating online treaty relevant games such as a "Where's Waldo" inspired challenge where individuals, using avatars to mask their identity, would be given points when they identify treaty relevant objects; another game challenged users to use geocaching and QR codes to accept and

[8] The Center for Geospatial Intelligence (CGEOINT) at George Mason University focuses http://cgeoint.gmu.edu/research.html

[9] Barry Costa and John Boiney, "Social Radar," MITRE Corporation, March 2012, http://www.mitre.org/work/tech_papers/2012/12_0581/

complete challenges from treaty experts.[10] Such games would be difficult to execute in the current environment, and indeed could have a negative impact if challenges were issued without the proper foundation. Absent a significant public education campaign, it is highly unlikely that the general public would be able to directly identify detailed verification tasks such as the movement of warheads or their associated support vehicles.

There appears to be a direct relationship between the complexity of a verification task and the level of expertise that would be required to complete the task. This suggests it might be more constructive to focus on identifying and engaging a network of outside experts analysts. Analysts from diverse disciplines have increasingly sophisticated tools at their disposal, and have the ability to self-mobilize in response to current events. For example, last year, North Korea paraded six road-mobile ICBMs through Pyongyang and experts from Arms Control Wonk posted a series of blog posts on whether the missiles were real, or simply aspirational mock-ups, and whether China violated sanctions and export control laws by selling the DPRK the Transporter Erector Launchers (TELs) that were seen in the parade. Missile experts, language specialists, defense analysts and people with expertise on a variety of other issues all weighed in, shedding light on what likely would have otherwise gone unnoticed.

Access to high quality commercial satellite imagery has also allowed outside analysts to provide additional insight and expertise by using this imagery to give the public a better understanding of what is happening in certain countries. For example, the Institute for Science and International Security (ISIS) utilizes satellite imagery to analyze nuclear sites and facilities in Iran, Syria, Israel, Pakistan, India and North Korea. Citizen “scientists” have also proven highly effective and accurate in projects coordinated by the National Archives, Galaxy Zoo, and National Geographic, to name a few.

How such analysis is corroborated and integrated with existing information structures and how outside experts are cultivated and connected will be important issues to consider if third party analysis is formally integrated in future frameworks. It might prove valuable to leave these communities separate from formal verification systems and allow them to act as both a check and balance to state-level analysis and a canary in the coal mine to identify areas requiring further attention by national authorities. In either event, such contributions should be taken into account when states make national assessments of treaty compliance. A formal integration mechanism may not be necessary, but at a minimum, outside analysis can serve as a cuing mechanism for analysts within government who have additional data resources at their disposal. Lessons learned from the safeguards and nonproliferation community should be considered in this context as the IAEA has been successful in integrating open source and third party information and analysis with Agency evaluations.

The Role of Government

Because governments are ultimately responsible for making arms control compliance determinations, they should have an interest in collecting and analyzing as much information as possible in order to make judgments. Yet the contributions that societal verification might make

[10] Childers A and Mappus R; *Innovation in Arms Control Challenge;* March 4, 2013; http://www.state.gov/t/us/205680.htm

in this regard are not well understood or accepted internationally. This is further complicated by the fact that governments have competing interests and policies on online access, freedom of speech and privacy. The effectiveness of societal verification is not just a matter of balancing security concerns with civil liberties, though that is certainly one key component. Governments that restrict access to the Internet and censor the content on certain sites can also impede the future prospects for societal verification contributions to the arms control and nonproliferation fields. Participation from non-democratic and less transparent governments will be very challenging, but is critical to the overall success of any future arrangement.

Some of the government actions that can affect societal verification efforts include:

- **Restricting Access**: In 2009, the Iranian government shut down online sites amid the Green Revolution. And in 2011, the Egyptian government shut down the Internet in an attempt to stifle the protests that were ultimately responsible for ousting Egypt's longtime ruler, Hosni Mubarak. If social media steams are shut down or seen as unreliable, it can affect the ability of the user to collect information when it might matter most.

- **Censoring Content**: The Chinese government has been widely criticized for censoring content and silencing activists with opposing viewpoints. The debate over freedom of speech and what can and cannot be said online has also caused some governments to intervene. Censorship could impact the quality and reliability of the information available, and if only partial information is collected, incomplete and erroneous conclusions might be drawn.

- **Protecting Privacy**: At least forty nations have enacted privacy legislation of some sort, either protecting internal, overseas, or both types of data transfers.[11] However, there is no overarching international law protecting internet privacy. In the United States, the Federal Trade Commission is continuing to work with its counterparts in the EU to put forward a consumer Do Not Track List and Privacy Bill or Rights, but it is not yet clear whether and how these mechanisms would apply to the national security domain. If citizens who have relevant information are concerned that their privacy or identity could be compromised, they may be unwilling to participate or share their observations or analysis.

Given the international character of the data and tools, international norms and arrangements could foster greater understanding and trust among governments with different legal and civil liberty policies. If states broadly decide societal verification has value, they may be motivated to enumerate the rights and responsibilities of users and consumers in future arms control treaties or agreements. A framework that clearly establishes the role and responsibilities of citizens, technology holders, states and international bodies is more likely to address legal concerns surrounding espionage and treason, since contributing to another state's all source intelligence collection may be perceived as such. Societal verification contributions will always be fundamentally unreliable as a stand-alone source given the prospects for government

[11] For a full list of internet privacy laws, see *http://www.informationshield.com/intprivacylaws.html*. Notably absent from this list are Russia and China.

intervention and manipulation, further reinforcing the notion that societal verification is a supplement to traditional tools and methods.

CONCLUSION

As the public debate on privacy and the role of government continues to unfold, proponents of societal verification need to better communicate what information can be collected, and for what purpose. Public-private partnerships focused on arms control and nonproliferation indicators may help work around the resource constraints facing existing open source collection efforts, and alleviate the mistrust and fear of a poorly articulated and less transparent government run effort.

Efforts aimed at mobilizing the general public to identify and relay treaty relevant information face many challenges. A more fruitful path might be to focus on creating a network of outside experts who already have both the interest and the relevant expertise, and create a pathway for those experts to communicate their analysis and observations to those in government who are ultimately responsible for determining whether a state is living up to its treaty obligations.

How to integrate information gleaned from such tools and sources into larger framework for monitoring and verifying a state’s nuclear activities is a long term challenge. By clearly articulating the responsibilities of all stakeholders and establishing global norms for use and conduct, states can start to leverage the power of new information and communication technologies in a more effective and systematic manner.