NUCLEAR MONITORING AND VERIFICATION IN THE DIGITAL AGE: SEVEN RECOMMENDATIONS FOR IMPROVING THE PROCESS

Nuclear Verification Capabilities Independent Task Force of the Federation of American Scientists

Third Report

September 2017

Monitoring and Verification in the Digital Age:
Seven Recommendations for Improving the Process

Nuclear Verification Capabilities Independent Task Force
of the
Federation of American Scientists

ABOUT THE TASK FORCE

The nonpartisan Nuclear Verification Capabilities Independent Task Force was convened by the Federation of American Scientists (FAS) to examine the technical and policy requirements for verifying a nuclear agreement with Iran. The Task Force published its first report in September 2014, outlining suggested requirements for monitoring and verifying a nuclear agreement with Iran. In its second report from August 2015, the Task Force outlined six achievable steps for implementation of an effective verification regime for the agreement with Iran. Although the Task Force was one of several groups making outside recommendations, several of the recommendations from our first two reports are similar to elements that have become part of the implementation of the Iranian nuclear agreement. (A complete list of recommendations from the Task Force's earlier reports can be found at the Task Force's project webpage.[1]) In this third report, the Task Force considers the growing capabilities and uses of commercial imagery, big data analytics, and social media reporting to examine how these trends could be combined to allow nongovernmental organizations (NGOs) to have a larger impact on the nonproliferation monitoring and verification community.

Acknowledgements

The leading members of this Task Force are Chris Bidwell, John Lauder, Harvey Rishikof, and Dr. Charles Ferguson, with significant help from FAS staffers Pia Ulrich and Frankie Guarini. In addition, Valerie Lincy and Matt Godsey from the Wisconsin Project on Nuclear Arms Control, as well as Melissa Hanham and Dr. Jeffrey Lewis of the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey, contributed research to this effort. During the course of this project, the Task Force organized several roundtable discussions: at Stanford University's Hoover Institution on War, Revolution, and Peace; at the William and Flora Hewlett Foundation headquarters in Palo Alto; at Harvard University's Belfer Center for Science and International Affairs at the John F. Kennedy School of Government; at The Citizen Lab at the University of Toronto's Munk School of Global Affairs; at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey; and at the offices of the Federation of American Scientists. Task Force members also met individually with experts both in and out of government. All in all, the Task Force members conferred with over 50 experts in the arms control, nonproliferation, verification, international law, and security fields, and considered their inputs in making these recommendations. We thank each of them for their contributions. The members of the Task Force would also like to thank the John D. and Catherine T. MacArthur Foundation for its generous funding of this project.

Disclaimer

This report is a product of the Task Force as a whole and not of the Federation of American Scientists, which simply convened the Task Force. The report represents the personal views of the members of the Task Force and should not be seen as reflecting the views of the private and government organizations with whom the Task Force members are now or have been affiliated, or the views of the individuals and organizations with whom we consulted.

Introduction

The goal of this Task Force report is to offer findings and make recommendations regarding nonproliferation monitoring and verification in general; our observations are grounded in large part on the Task Force's continued attention to the Joint Comprehensive Plan of Action (JCPOA) between the P5+1 and Iran, nuclear developments in North Korea, and other nonproliferation challenges.

The Task Force seeks in this report to examine some of the significant developments in the current digital age as they relate to nonproliferation monitoring activities by both governmental and non-governmental organizations (NGO), to include:

1. the accelerating quality and quantity of available imagery and other forms of remote sensing available outside governments;

2. the growing volume and availability of worldwide transactional data related to commerce; and

3. the ease of communicating findings, observations, and assertions about illicit activities related to nuclear programs and proliferation (with varying degrees of accuracy and truthfulness) through an increasing number of traditional and newer social media outlets.

Overlaying these three developments is the introduction of new forms of data analytics, including nascent artificial intelligence (AI)[2] approaches such as machine learning, which serve to speed up both the process and pace at which these developments affect monitoring and verification activities. The sheer volume of available data, imagery, and analysis, some of it conflicting, has made the nuclear monitoring (data gathering) and verification (a policy determination ideally based on accurate data) more challenging due to a significant worsening in the signal-to-noise ratio.[3] Additionally, as all three of these developments reflect modern society's dependence on the digital cloud, servers, data storage, websites, and internet communications, the need to ensure data integrity has increasingly become a salient concern.

Enabled by these increases in the speed and quantity of open data sources, the NGO community will play an increasing role in commenting on the JCPOA and other nonproliferation agreements, in facilitating greater transparency, and in helping to identify options, opportunities, and challenges. Use of these enhanced open-source tools by the NGO community is likely to increase as the technologies continue to improve and costs continue to decline. A paper co-written by Dr. Christopher Stubbs of Harvard University and Dr. Sidney Drell of Stanford University, titled "Public Domain Treaty Compliance Verification in the Digital Age," described these new tools collectively as "Public Technical Means (PTM)."[4]

The intent of the findings and recommendations of this Task Force report is to suggest some of the measures that could be taken to enable the work of nongovernmental bodies in nuclear monitoring. The report highlights a few of the many examples of additional analytical and information resources available to NGOs. The report further suggests ways in which relevant analysis and reports can be separated from misinformation, and ways in which transparency can

be enhanced. The findings and recommendations are not intended to be comprehensive but rather to suggest some possible measures as illustrations of what might be possible and how to exploit these new tools.

The report examines examples in the human rights and business communities where centers for facilitation of monitoring activities and for validation of claims have been established independent of advocacy groups and governments. Our report calls for the establishment of similar centers focused on fusing and authenticating arms control and nonproliferation information. In the governmental arena, the report calls for more openness and better publicizing of the cooperative efforts of all parties working to ensure Iran's compliance with the JCPOA. The final set of recommendations focuses on methods for maintaining the integrity of monitoring data as well as the safety and privacy of people who are working on ensuring compliance with nonproliferation objectives. A short summary of the recommendations follows:

1. An independent Network of Centers of Nonproliferation Authentication (NCNA) — a distributed network consisting of four to five separate institutions worldwide — should be created and funded outside of government and advocacy channels.

2. The P5+1 and Iran should seek opportunities for public ceremonies, press coverage, and diplomatic events to mark important implementation steps.

3. There should be periodic public updates on monitoring measures and U.S. support to the IAEA and the Joint Commission.

4. There should be a priority diplomatic push by members of the P-5+1and other interested states, supported by the international business community, toward encouraging Iranian openness and more public release of data concerning implementation and compliance steps by Iran.

5. A trusted body of outside experts should be created for the Iranian nuclear agreement to review monitoring efforts and build confidence even among skeptics that serious and appropriate monitoring steps were being taken.

6. NGOs, in the nonproliferation and nuclear arms control sectors that are collecting, handling, processing, and storing sensitive personal information, should take the necessary actions and use appropriate tools to protect both the information and the physical safety of its providers.

7. Funders of nonproliferation NGOs should consider robust funding for upgrades in cyber security in order to protect key data and should insist that fundees adopt a culture of maintaining good "cyber hygiene" by their personnel as a condition of receiving grants.

BACKGROUND AND CONTEXT

Implementation of the Iranian nuclear agreement is at an important milestone in nonproliferation monitoring and verification. In July 2017, the U.S. Department of State again certified that Iran is meeting its obligations under the JCPOA. The IAEA reports that Iran appears to be complying with the letter of the agreement concerning fissile material production, yet other concerns persist. The missile test activities and the alleged creation of additional underground facilities for Iran's missile program may even suggest a continued focus on creating the capacity to deliver nuclear weapons at some point in the future. Significant questions also remain about how far the design of nuclear weapons and weaponization efforts may have progressed in Iran, and whether such work could continue in some form even as the JCPOA remains in force. Complicating Iran's desire for more robust sanctions relief are the issues of Iranian support to the Assad regime in Syria, support to various destabilizing terrorist groups in the Middle East, suspected human rights violations, and alleged cyberattacks. These activities are of continuing concern and form the basis for non-nuclear U.S. economic sanctions outside of the parameters of the JCPOA.

The Trump administration, Israel, Saudi Arabia, and other Gulf regional states are pushing back against Iranian behavior. The United States has announced new potential arms sales to the region designed in part to counter Iran. The United States has also imposed new sanctions on Iranian and other entities related to Iran's ballistic missile program. There is a current debate within the U.S. Administration regarding the future of the JCPOA. The National Security Council recently announced that it is leading an interagency review of the JCPOA to determine whether the lifting of sanctions resulting from the agreement is consistent with U.S. national security.[5]

The results of the Iranian election in May 2017 might provide an opportunity for more forceful international discussions. Iranian President Rouhani won reelection, in part, because of his commitment to advancing the Iranian economy, but economic improvement will largely rest on convincing Western companies that Iran is a stable and reliable trading partner. That would likely require some moderation of Iranian behavior, greater transparency, and a more favorable business climate in Iran. At the same time, Rouhani, with a successful reelection behind him, may have some additional negotiating room for Iranian moves to allay Western concerns.

The JCPOA itself provides a venue for discussions of broader security issues. How the agreement's Joint Commission could serve as a forum for such negotiations was discussed at greater length in Recommendation Four of the first Task Force report. The Task Force will have more to say in its subsequent work about how the Joint Commission could enhance communication on tough issues and serve as a forum for raising possible additional confidence-building measures among the parties.

This monitoring and verification environment is significantly different than the information and communications environment of some 55 years ago, when satellite imagery was first used for purposes of monitoring nuclear weapons threats and was the exclusive province of the two superpower governments of the day: the United States and the Soviet Union. The images derived from those early systems were often infrequent, grainy, and low-resolution, requiring highly sophisticated expert interpretation and analysis. Additionally, data concerning the details of the process and progress of states creating new nuclear weapons, and where they were being built,

was largely obtained through clandestine methods. Consequently, the various analyses by governments of what those images and documents meant were some of the most closely guarded secrets, rarely shared or seen outside of official channels. When information was released, it was reported by professional news organizations and was often filtered through a series of seasoned editors. Fast forward to today, and the environment for imagery, data, and distribution is radically different. This has significant implications for the prominent nuclear threats of today.

A RECENT CASE STUDY HIGHLIGHTING THE NEW CHALLENGES

As was recently seen in the lead-up to the negotiation of the JCPOA agreement between Iran and the P5+1, various NGOs attempted to play an outsized role in influencing both sides of the debate surrounding the establishment of the agreement. An example of this was seen in the case of a claim made by a group calling itself the National Council of Resistance of Iran (NCRI). On February 24, 2015, NCRI held a briefing at the National Press Club in Washington, D.C., where it presented a case — supported by overhead imagery — that there was a previously undiscovered and unreported underground centrifuge lab at a location inside Tehran known as Lavizan-3.[6] The allegation was particularly well-timed, as it was announced on the same day that Secretary of State Kerry was testifying on Capitol Hill regarding the status of the negotiations with the P5+1. He was asked questions about the new allegation during his testimony. This all happened just six weeks before the parties agreed to the JCPOA. In the days that followed, the claim was widely debunked by a few bloggers using open-source materials and different imagery, including Dr. Jeffrey Lewis of *Arms Control Wonk*. Still, the State Department could only say that they were investigating the claim. Interestingly, one United States senator was still referring to Lavizan-3 as a legitimate target for inspection and investigation some two and a half months later.[7]

As the saying goes: "A lie gets halfway around the world before the truth has a chance to get its pants on." Currently, the inability to separate fact from fiction greatly affects the proliferation monitoring communities, both governmental and nongovernmental. The result is a worsening in the signal-to-noise ratio regarding information on suspected illicit nuclear weapons programs. The Task Force has examined this new environment and reached findings that will hopefully benefit analysts and nonproliferation experts as they deal with and account for these developments. The JCPOA brings a sense of urgency to addressing this data proliferation, as claims and counterclaims regarding the parties' compliance with the JCPOA, as well as other proliferation challenges, are expected to grow.

ADDRESSING THESE DEVELOPMENTS

Given the evolving data environment, it is important to think about the strategic implications for policymakers at the most senior levels of government. Traditionally, most governments have processed and distributed suspected proliferation information largely within classified channels (including judgments about the credibility of information obtained through open sources). However, the expanding public NGO sector now has the tools (PTMs) to produce compelling analysis with competent supporting evidence that can offer competing narratives regarding compliance or noncompliance with nonproliferation obligations.[8] Because of the growing number of new media and social media sites, alternative narratives can easily gain traction in

public debates and therefore must be accounted for by policy leaders. The standard for such public narratives gaining policy traction is not necessarily that they are true, but rather that they are merely plausible. Consequently, such alternative narratives will be factored into policy debates among senior leaders, as was the case with the Lavizan-3 reporting. Even in non-Western or non-democratic countries, these public narratives must still be addressed by leaders as they may form the basis for calls for sanctions, economic boycotts, diplomatic pressure, and even military action by outside countries. Of note, such negative narratives may provide an impetus for noncompliant states and other actors to create and spread false counter-narratives.

Understanding the reach and influence of this new open monitoring environment is important not only for increasing public awareness or academic research purposes, but also for informing those individual advisors closest to the key policymakers. Grasping the significance of how proliferation threats are publicly monitored and reported is a crucial step in formulating and implementing effective policy — not only to detect illicit activity, but also to avoid getting fooled by spurious claims.

THE TASK FORCE'S APPROACH

The Task Force focused on three important communities that are affected by these new phenomena and has made some recommendations on how analysts and policymakers might collectively adapt to the new environment when sorting through well-grounded facts, mere plausibilities, and unsupported assertions. Those relevant communities are:

1. the NGO nonproliferation community,

2. the U.S. and other governments' nonproliferation and monitoring organizations and ministries (as well as international bureaucracies such as the IAEA), and

3. the broader nonproliferation NGO enabling community (funders, citizens, investigators, reporters, raw data providers, technical support, internet privacy and network security providers).

The first section of this paper will outline developments and the state of the art for imagery, trade databases, analytical tools (including artificial intelligence), and media distribution (social and traditional) as they currently affect nonproliferation monitoring and verification challenges. The next three sections examine and make recommendations on how the above listed three groups can adapt to this new digital environment.

[This page intentionally left blank.]

Section I – State of the Art for Imagery, Data Analytics, and Media

Before beginning a discussion on the use of technological tools useful in today's nonproliferation and verification environment, it is instructive to briefly examine the history and the current state of the art for some of these new technologies:

1. Tracking Proliferation Threats Through Commercial Overhead Sensing Technologies[9]

The usefulness of examining a situation from above is an intelligence gathering concept that has been used throughout the ages. During the Cold War, the United States and the Soviet Union sought to view each other's nuclear delivery arsenals from space. The Cold War approach of gathering data from overhead monitoring tools has remained a mainstay for the major international powers with continuing technical improvements in sensor types and greater image resolution. A major change has been the increase in the sheer number of available observation platforms and, more importantly, the availability of remote sensing data to the general public at a very low cost, or even free in some cases.[10] The first overhead satellites used for collection of knowledge and data were launched into space through government sponsorship, managed and controlled by major government powers (mostly the United States and Soviet Union) and initially could only produce low-resolution images that were rarely released to the public. Currently, and into the foreseeable future, a significant number of satellites in orbit will be owned by private entities and will produce data from various overhead sensor devices, including optical and multi-spectral. Unlike legacy aerospace firms that focused on national security clients, these newer private firms are financially incentivized to sell their products to as many customers as they can, including governments. This does not mean that large governments will not have their own highly capable and often classified capabilities providing exquisite and detailed data uniquely suited for monitoring illicit nuclear activities. However, it does mean that governments are no longer the exclusive or predominant source for overhead data, which has implications for verification policies and activities related to nonproliferation goals.

The global commercial satellite imaging market is growing rapidly, and is projected to surpass $6.4 billion by 2023.[11] The current marketplace for overhead imagery is comprised of a growing number of U.S. and foreign companies selling both high resolution satellite imagery as well as data derived from smaller, medium-resolution satellites. Most providers of overhead imagery do not only sell archival satellite imagery, but also allow for tasking a satellite to obtain imagery from a desired site. Prices for tasking can be as low as $24 per square kilometer — with a minimum order area for new tasking collections of 100 square kilometers.[12] Notable suppliers of satellite imagery data include Digital Globe, Airbus Industries' Defense & Space, and the U.S. government's Landsat, which also provide imagery for mapping sites such as Google Earth Pro,[13] Google Maps,[14] Bing Maps,[15] Yandex Maps,[16] Here,[17] and Baidu.[18]

A comparatively recent development is the lower cost deployment of smaller, lightweight satellite systems with lower resolution. Large satellite constellations allow for increasing global imaging coverage with more frequent revisit rates. A relative newcomer to the commercial satellite business that follows this approach is Planet. As of the time of this writing, Planet has launched approximately 150 medium-resolution satellites (called Doves), which will soon provide pole-to-pole imagery of earth on a daily basis.[19] Imagery derived from these smaller

satellites serves to identify potential issues and areas of concern. Analysts can then follow-up by tasking higher-resolution satellites to examine specific sites in more detail.

Other noteworthy recent developments enable analysts working with satellite imagery to integrate overhead data with mapping/content services. Additionally, advances in technologies and techniques for analyzing imagery data allow for the relatively rapid processing of raw satellite data into useful contextual knowledge.[20]

More detail on this subject can be found at the Task Force's project webpage.

2. Tracking Proliferation Threats Through Trade Data Analysis

An increasingly significant monitoring tool used by nonproliferation NGOs involves the examination of trade-related data (e.g., import declarations, export declarations, tenders, customs reports, transportation manifests) to look for indications of technology transfers related to nuclear weapons production, or for transfers involving entities linked to such production. This is significant as clandestine proliferators often utilize the tools of legitimate commerce (e.g., banking, insurance, transportation) in the process of acquiring dual use items. The challenge in looking for evidence of nuclear proliferation in all of this transactional trade data involves finding that handful of documents related to specific transactions of concern. The key documents will often reside in a vast universe of legitimate trade data. Twenty years ago, finding such documents was a slow physical process. To obtain key documents, an individual analyst was required to visit a large bureaucracy or company to sift through paper records and/or microfiche to find records of specific transactions. Such efforts consumed extensive time and person-power. In more recent years, data derived from export declarations at national customs agencies has become more readily available and affordable through commercial services and is available electronically through the Internet. Trade data can take the form of transactional data, which includes specific information about individual transactions, and statistical data that tracks trade flows. The electronic sources include government documents, customs declarations, bills of lading, and other documents related to imports and exports.

Today, subscription services often collate and hold import and export data. However, the type and quantity of the information provided, as well as its subscription price, vary widely. Monthly subscriptions to services allowing individual queries of trade data range from approximately $100 (Import Genius: last three months of U.S. import data only, limited to 10 searches per day) to more than $600 (Datamyne: last two years of U.S. import and export data, unlimited searches with the ability to export several thousand lines of data with each search). The least expensive subscription plans usually are limited to a subset of data, often only from a single country, or for a brief period of time. Some providers offer daily updates (Datamyne, IHS/PIERS, Panjiva) sourced from U.S. Customs data; access to international trade data through these providers can take as much as two months. Differences also exist with regards to archival data, which may require premium subscriptions, may be restricted to U.S. data only, and generally does not precede the year 2004. Providers also offer useful resources created by collating the millions of bills of lading in their databases, such as company profiles for individual shippers and exporters. This feature makes it possible to view a summary of a company's full trading activity, a breakdown of the export markets it serves, and a description of the goods in which it trades.

In addition, it is possible to purchase bulk trade data from commercial providers, for incorporation into another system that allows for the application of data analytics and machine learning tools, such as a queuing function. In this way, trade data can be combined with other information (corporate registration, vessel movement, satellite and sensing, etc.) for network or trend analysis, and other data manipulation. However, the cost of such bulk purchases is significant and varies based on use (e.g., $25,000 for six months of some U.S. export data). The terms and conditions may also limit how widely the data can be shared.

Trade data providers may supply a number of data elements for each transaction, including bill of lading number, vessel name, International Maritime Organization (IMO) code, voyage number, carrier line, consignee name and address, shipper name and address, ports traveled through, product/cargo description, product HS code, cargo weight, and port of origin and destination. There may be differences in the level of detail provided for certain data elements depending on the country from which the data is drawn. For example, for a shipment from Peru to Ecuador, the name and address of both the shipper and consignee would be provided, along with a detailed cargo description as submitted by the shipper. However, for an export from China, only the name and address of the shipper and the country of destination would be provided, along with an HS code number/description for the cargo, which can often cover a broad category of goods rather than a specific item.

Commercially available trade data is, and has been, used in tracking proliferation by several arms control organizations and nonproliferation experts. The Wisconsin Project on Nuclear Arms Control, for example, reviews transaction-level information to identify a company's suppliers and/or customers, the countries or regions in which the company is active, what products or commodities it trades, and what names and addresses it uses when conducting business. This information is used to create individual profiles of entities of concern, which comprise the Risk Report, a database with nearly 5,000 entities of concern for proliferation. The project has used Panjiva, as well as a resource called Trade Navigator (both subscription services providing import and export data), and has uncovered several instances of sanctions violations.

Additionally, King's College London's Project Alpha focuses on researching illicit trade in support of the nonproliferation regime. In one particular project, Project Alpha's researchers used trade data to analyze Pakistan's procurement network for dual-use goods; they identified a network of at least 20 trading companies in China, Hong Kong, Dubai, and Singapore.[21]

More detail on this subject can be found at Task Force's project webpage.

3. Use of AI and Machine Learning to Analyze Overhead Sensing and Trade Data

One of the classic methods an organization can use to process more quickly raw and unstructured data is to develop or hire expertise in a particular area of interest (such as nuclear weapons programs). Given the current exponential growth in the amount of nonproliferation data to be reviewed and analyzed, finding a cheaper method of collecting and sorting through that data has become an important imperative. This is why emerging machine learning techniques are quickly becoming more relevant to both the governmental and NGO nonproliferation communities. AI

offers the ability to collate and fuse large amounts of unrelated data sets (such as imagery and shipping manifests) and see relationships. Some examples of how AI use is evolving can be found on the website of a company called Black Sky,[22] which focuses on two major capabilities; imagery and insights. While Black Sky's imagery offer allows users to discover, purchase, and download high-resolution imagery from 16 satellites, the company's goals for 2020 are to provide intra-hour revisits in popular areas that will be made available to customers within 90 minutes of completing their order, regardless of the customer's location and time zone — for a mere $90. Black Sky's insights capability fuses satellite imagery with other data sources, such as social media and news feeds, and allows users to search for themes (e.g., geopolitical conflict, energy, natural disaster), or obtain data feeds curated by location (e.g., port, pipeline, border). In this case, an algorithm could end up doing the majority of the traditional analysts' laborious grunt work. The implications are twofold: First, the analyst (government or NGO) can run the algorithm against more leads or tips ensuring that fewer indicators of illicit activities are missed or overlooked. Second, the capability gives the NGO and government analysts using AI and machine learning the ability to bring their concerns to policymakers more quickly and with significantly more detailed evidence.

More detail on this subject can be found at Task Force's project webpage.

4. Publicizing Suspected Proliferation Through Traditional and Social Media Outlets

Techniques for sharing knowledge, information, and opinions have evolved throughout the years. Each new technique tends to increase the number of people receiving a particular piece of information and the speed at which that information can be distributed. Such was the case with the introduction of radio and television. With the advent of internet communications and social media outlets, the ability to amplify a narrative among billions of people (whether or not it is complete, accurate, or an outright falsehood) occurs within a highly compressed timeline. For some people, it takes only a couple of seconds and a couple of clicks to spread a tweet around the world to billions of people. The evolving impact of rapid communications needs to be appreciated in the context of identifying and calling out illicit nuclear programs, as well as for dealing with propaganda battles that accusations of illicit nuclear activity can spawn.

In the Western world, Facebook sits atop the list of the most popular social networking sites with an estimated 2.1 billion monthly active users in June 2017.[23] It is followed closely by YouTube with an estimated 1.5 billion users per month;[24] Twitter is a distant third with 328 million unique monthly visitors.[25] On a global scale, however, the social media landscape is surprisingly diverse. Different parts of the world favor different social media platforms, reflecting both preferences and circumstances, and more importantly what gets seen or not seen.

For example, Western social media favorites Facebook and Twitter are blocked in China in what has been called the "Great Firewall of China." While there are ways to skirt such blocking, indigenous Chinese social media platforms Sina, Weibo, and Renren have filled the gap and become the Chinese equivalents of Facebook, while Qzone has replaced Twitter. Chinese users rely on Tencent, QQ, and WeChat for mobile communications and private social networking, while Youku and Tudou replace YouTube. Mostly unknown and hardly used in the West, these platforms generate large user numbers in China, the world's most populous country with about

1.38 billion people. QQ alone has more users than the overall users of LinkedIn, Twitter, and Instagram combined. The estimated number of Chinese active social networking users is twice the population of the United States (which has about 323 million people).[26]

Similarly, users in Russia and many Russian-speaking former Soviet states prefer Vkontakte (VK) and Odnoklassniki over Facebook. As of 2017, VK has more than 420 million users, and is ranked fifth on a list of worldwide websites with the most traffic;[27] Facebook, in contrast, is only used by 13.7 percent of Russian internet users.[28] Interestingly, Ukraine just banned VK and Odnoklassniki in an effort to shake off Russia's influence. As a result, millions of Ukrainians are now using Facebook instead.[29]

In other countries, such as India, the social media revolution is still waiting to happen. 28.4 percent of the Indian population (about 1.32 billion people) is using the internet. While social media use continues to grow and has reached growth rates of 26 percent from 2014 to 2015, in 2016 only 10.3 percent of Indian internet users were active on social media.[30] It is predicted that, even at this rate, it will take another 16 years before half of all Indians will use social media. Among the Indian social media users, Facebook is the most browsed social network, attracting 83 percent of internet consumers.[31] However, it should also be noted that the sheer number of competing communications channels that support a multitude of individual political parties, especially in India's democracy, can negatively impact debate on policy issues as they compete with each other to be the most outrageous and bombastic.[32]

While social media users in the Middle East use Facebook (88 percent in 2013) and Twitter (45 percent in 2013), use thereof has fallen in recent years, whereas Instagram's popularity has exploded from a mere 6 percent in 2013 to 28 percent in 2015. WhatsApp (77 percent) and YouTube (54 percent) are now dominant social media platforms. A 2015 survey found that individuals that felt less comfortable expressing political opinions were also less likely to use social media, and people who feel comfortable voicing political opinions online use more social media. A 2017 survey indicates that where government monitoring is a concern, WhatsApp is the preferred source of news.[33] This may be attributable to the fact that current versions of WhatsApp are free and include end-to-end encryption.

In June 2016, Iran had 56.7 million internet users (more than 68.5 percent of the population). In a 2012 study, 58 percent of Iranians were found to use Facebook regularly despite restrictions imposed by the Iranian government. In 2016, Facebook remains among the most popular social media platforms, despite still being blocked.[34] However, 69 percent of the Iranian youth use Virtual Private Networks (VPN) to bypass the government's filtering. Instagram seems to have been fitted with "intelligent filtering," but is currently not blocked, with the exception of criminal and immoral content. Celebrity Instagram accounts are also not accessible without VPN connections. Nonetheless, Instagram is reported to be the most popular social media platform in Iran.

In Africa, a number of governments (among them Uganda, Congo, Chad, Burundi, Zimbabwe, and Ethiopia) block access to social media sites in their countries, including WhatsApp, Twitter, and Facebook. In 2014, 100 million people were using Facebook each month across the continent; that number grew to 120 million users in 2015, with 15 million users in Nigeria, 12 million in South Africa, and 4.5 million users in Kenya.[35]

As these above referenced social media silos develop among significantly sized populations, it is logical to assume that users will be sharing "alternative facts," developing different contextual realities, and generating counterfactual narratives regarding foreign policy and security concerns, including nonproliferation. Influencing public opinion in this environment is increasingly difficult and hard to manage. Knowing who the influencers are in these communication silos and breaking through them is an important first step in shaping the conversation. To that end, Graphika has entered the market as a private sector company that analyzes social media data seeking to identify community-specific influencers, content, and conversations. Graphika leverages proprietary social network analysis and graph mathematics from Twitter and other public sources, to identify networks of influence, and the content shared therein, to trace how information travels among social networks. Partnering with the Berkman Center at Harvard, they have produced reports such as "Beyond the Wall: Mapping Twitter in China," analyzing how Chinese users circumvent content restrictions and maintain global connections outside the government sanctioned networks.[36]

More detail on this subject can be found at Task Force's project webpage.

Section II – Findings and Recommendations Regarding Monitoring Activities in the NGO Nonproliferation Community

Context

In the aftermath of several elections around the world increasingly, "fake news" is now big news. Today, accidental misinformation, disinformation, and deliberately falsified propaganda are widespread and have gathered significant traffic on the Internet.[37] Much of this information is reportedly coming from Russian state-sponsored sources, including automated "bots with an agenda" that can mask their Russian roots. There is a fear that malicious actors may continue to flood American news with propaganda. Both foreign powers and domestic organizations have been able to harness the power of fake news to distort an individual's view of information, with potentially significant ramifications for policy and state action. The proliferation of NGOs and unsubstantiated facts from questionable sources can have a significant impact of the ability of policymakers to make informed verification judgments.

Commentators in the mainstream press have mixed views on this issue and on the potential ways to screen for fake news, some urging the involvement of private corporations like Facebook, while others look to national governments. Facebook, after its internal investigation on political ads in the 2016 U.S. election, removed approximately 470 accounts. However, fake news is not necessarily a new issue. Falsified news reports have been used for hundreds of years for political purposes, from the infamous anti-Semitic conspiracy theory "The Protocols of the Elders of Zion" to stories sponsored by revolutionaries to increase anti-British sentiment during the American Revolution.[38] Still, with the modern prominence of the Internet and social media, it is much easier for those who create misinformation to spread their ideas to a wider audience. Their potential influence is becoming more profound and disturbing due to scale and speed.

In the nuclear proliferation realm of monitoring and verification, the fear of having "fake" photographs (as discussed in the Lavizan 3 case, supra) or false documents to influence a policy debate is particularly troubling and, given the acceleration of news cycles, increasingly a threat. As Sabrina Tavernise discussed in a recent *New York Times* article:[39]

> The larger problem, experts say, is less extreme but more insidious. Fake news, and the proliferation of raw opinion that passes for news, is creating confusion, punching holes in what is true, causing a kind of fun-house effect that leaves the reader doubting everything, including real news.

One challenge for policymakers is to make decisions amid all this noise. The need to break through the noise with facts that can be agreed on by most people is necessary if rational policy is to be developed and executed. The technical nature of illicit nuclear threats makes doing so a difficult challenge, not unlike the current controversy circulating around climate change policy.

Another challenge is presented by the changing nature of what modern society considers to be knowledge or truth. Expertise is no longer confined to individuals with deep knowledge of a particular subject, but rather the merged knowledge of the collective crowd, all of whom bring different training and experiences to a particular problem. In other words, the smartest person in the room is now "the room" itself. While this crowdsourced approach to analyzing proliferation

threats has its advantages, relying on this approach can dilute accountability, which makes establishing the basis for a verification judgment, call harder to dissect, explain, and support with evidence.[40]

Key Findings

Increasingly policymakers must address the issue of "fake news" or competing narratives designed to influence attitudes, shape public opinion, and structure debate. The more technical the subject matter, the more difficult this task is to establish ground truth. With regard to nonproliferation specifically, one way to counter this emergent news area is the creation of nongovernmental sources to authenticate information that can be seen as impartial in either verifying true claims or countering false data.

Progress has been made on this problem in both the human rights and business arenas. Organizations like Bellingcat routinely monitor the crisis in Syria from human rights, conventional military, and chemical warfare perspectives.[41] The perception of credibility assigned to Bellingcat comes from their meticulous attention to detail and use of a multitude of images taken over time to create computer-modeled simulations that can tell a compelling story. It also stems from the fact that Bellingcat reports on legitimate human rights violations and also calls out fake reports with the same attention to detail and with a perceived independence from government influence. This gives Bellingcat's brand a presumption of integrity. Furthermore, the American Association for the Advancement of Science (AAAS) has created a robust, well-funded effort called the Geospatial Technologies and Human Rights Project that offers a range of modern tools, such as satellite images, geographic information systems (GIS), and Global Positioning Systems (GPS) that allow for mapping and analysis of multiple layers of geo-referenced data.[42] Data derived from this project is used by NGOs to advance effective social justice and environmental issues and concerns.

In the proliferation field, one activity close to AAAS and Bellingcat's success is the work of a few scholars at the James Martin Center for Nonproliferation Studies (CNS) in Monterey. They have been particularly successful in tracking developments in North Korea and Iran and are leaders in tracking and reporting on proliferation developments with precise detail relying only on publicly available data. They have also established a new crowd-sourcing project called geo4nonpro.[43] Other NGOs, such as 38 North[44] and Institute for Science and International Security,[45] also perform impressive work in this space. Yet, as is the case for many such efforts, the problems being addressed, as well as their consequences, are bigger than the resources available and may depend on individual passion rather than institutional stability and support.

Finally, as part of this project, a visit was made to Citizen Lab that is part of the Munk School of Global Affairs at the University of Toronto in Canada that looks at the intersection of Information and Communication Technologies (ICTs), human rights, and global security. The Citizen Lab monitors, analyzes, and helps shape the exercise of power in cyber space. The lab has been a model for bridging the "geek-wonk" intellectual and cultural divides. It combines both skill bases under one roof for its reports and judgments.[46] Citizen Lab, like the CNS and AAAS, works at separating fact from fiction and has many of the characteristics and attributes that would be applicable to forming a similar organization focused on proliferation concerns.

It should also be noted that the information integrity problem is not limited to components of the international security community. For example, at the Oxford Internet Institute scholars have tracked how bots have been used to spread propaganda via social media to influence elections. Or consider the group Politifact, a fact-checking website that rates the accuracy of claims of elected officials. There also is a long-established need for unbiased data and opinion in the business and banking communities. Investors in corporate bonds rely on independent analysis of bond rating agencies such as Standard and Poor's, Moody's Investors Service, and Fitch Ratings. Their value stems from the independence of the rating operations, sales, debt, and public statements in promotion of the business. When that independence was undermined prior to the 2008 Mortgage Crisis, the consequences were dire for the financial system.

Recommendation

Drawing upon the Citizen Lab model, the Task Force recommends the creation of a Network of Centers of Nonproliferation Authentication (NCNA) — a distributed network consisting potentially of four to five separate institutions worldwide as a beginning to reinforce a new research ethics paradigm. Once established, each center needs to be sufficiently funded. For prototype purposes it may be beneficial to establish a single operating center that could develop best practices and serve as a model to then be replicated.

As an "ideal type" each institution within the NCNA should include the following characteristics to establish the appropriate research ethics:

- **An arm's length relationship with governments or commercial sponsors**: Independence is essential to the believability of any successful arbiter of fact. If there is a hint of government funding or collusion in any one center, the NCNA's credibility would be undermined. Furthermore, setting such an institution up as a profit-making enterprise could also taint the credibility of the analysis. The burden for creating a network like this would undoubtedly require a large endowment or a sustained commitment from a major grant distributing institution or a private sector participant with an interest in the promotion of neutrality.

- **Academic institutionalization:** A large academic institution could appropriately take the lead role in creating a center for the NCNA. Each center would preferably be led by a tenured professor as that individual would be secure enough in his or her position to make impartial judgments and produce neutral analysis and have a stake in maintaining an academic reputation. Furthermore, housing the NCNA's leadership in a large academic institution would likely give quicker recognition and validity to its efforts within the nonproliferation policy community and the public at large. Moreover, the potential use of undergraduates and graduate students would help create the next generation of cyber investigators.

- **No role in advocacy:** Many institutions and individuals active in advocating for nonproliferation actions and policies may want roles in such a center. Unfortunately, that could be counterproductive to the requirement for independence, which is an absolute prerequisite for establishing credibility. Independent credibility can also be established through well documented reports, publications of a research methodology manual, and

stringent requirements for data and evidence resourcing.

- **Sources and methods transparency:** In order to ensure credibility and a commitment to impartiality, any published products, all significant sources of information, whether they support an analytic judgment call or not, need to be openly cited and published. Additionally, the NCNA can be a vehicle for merging multiple sources of geospatial data and trade data to produce comprehensive analysis of suspected illicit nuclear activities. Finally, in situations where time permits, the NCNA's analytic products should be peer reviewed by independent experts and commentators. The methodology must be transparent and open for review and criticism by the community.

- **Rigorous documentation:** To maintain credibility, all NCNA assertions and analytic products must have factual basis supported by documents, imagery, and recordings. Political and diplomatic judgment calls (verification) cannot be made by the NCNA but can be made by the readers of the reports, including government officials and NGO representatives. The goal of the NCNA would simply be to produce impartial analysis fully supported by all relevant facts. In effect, the NCNA would act like an umpire — calling "balls" and "strikes."

- **Serve as a resource to the nonproliferation community at large:** The NCNA should be nimble and responsive to the many small nonproliferation NGOs that do not have the technical capacity to do sophisticated analysis. By serving as a resource, the NCNA can be a central gathering point for processing and fusing crowdsourced information. Furthermore, the NCNA should be capable of training and sustaining a cadre of on-call geospatial and other analysts.

- **Foster active integration into faster news cycles:** The NCNA should make an effort to conduct outreach and become known by general media organizations so that in time of crisis they will be actively engaged in providing trusted expert analysis.

An important aspect of the center and centers would be a protocol for screening which issues would be selected to require such a rigorous process. Part of the center's mission statement would be to establish the criteria for investigation. It is envisioned by the Task Force that if this network proves to be successful, this framework might be useful for other public policy issues by bringing together subject matter experts with the resident and existing technical expertise of the centers. For example, some scholars have suggested that social media companies could maintain a database of campaign advertisements that appear on their sites, so they could later be studied for authenticity and accuracy in the election process. These centers would be the ideal locations for both storage and analysis of the ads. In short, the Task Force contends there are many possibilities for the NCNA framework if the proliferation prototype center proves to be effective.

Section III – Findings and Recommendations for the U.S. and Other Governments' Policymaking Communities

Context

The growing capabilities of NGOs, as significant as they are, do not diminish the primacy of governments in monitoring and, more importantly, in making verification determinations, which can only be performed by governments. Governments have a far greater capacity — largely through intelligence sources and methods, as well as negotiated inspection, information sharing, and confidence building measures — to discover and penetrate nuclear weapons programs of concern. Governments too are well-positioned to encourage and facilitate the work of international organizations and NGOs to participate in the monitoring process and to attest to the credibility of verification judgments.

In this regard, however, the implementation of the Iran nuclear agreement has actually made it harder for NGOs, other observers, and governments outside those that negotiated the agreement from contributing to the monitoring process and from making judgments about the effectiveness of the agreement. The Iranian government has apparently argued strongly for confidentiality of nearly every aspect of implementation. Iranian concerns about public disclosures about the details of the agreement's implementation seem to arise from contentious Iranian internal politics about the agreement and a desire to maintain ambiguity and flexibility about past nuclear developments, agreement implementation steps, and future commitments.

The P5+1 and the IAEA have acquiesced in the Iranian penchant for secrecy both to secure an agreement and also possibly because of controversy about the agreement within participating countries and parts of the international community. The P5+1 and the IAEA are apparently receiving information relevant to the agreement from Iran. Agreeing to hold that information confidentially and not to provide details to other governments and the public was a relatively painless carrot to grant Iran in the negotiation.

Still, the lack of transparency and authoritative official reporting on the implementation of the agreement and compliance with it has created an environment in which suspicions, "fake news," and unfounded accusations can flourish.[47] This complicates the ability of both proponents and opponents of the agreement from making their case in the public political fora in which verification judgments are defended. There may also come a time when there may be a serious allegation on noncompliance that leads to a U.S. response that would require informed public and congressional support. The Task Force offers the following findings and recommendations to bring about greater transparency and to build greater confidence in implementation of the nuclear agreement.

Key Findings

Unlike the precedents of most prior arms control and nonproliferation agreements, there has been little public fanfare over the achievement of agreement milestones and of the implementation of monitoring measures. Both proponents and opponents of the agreement have shied away from publicizing the agreement's milestones and the ongoing important work of the Joint Commission is barely acknowledged. There also appears to be limited public understanding of the steps the United States and others are already taking to facilitate monitoring of the agreement. Lack of

visibility does not engender confidence in compliance or provide a basis for further steps. The lack of transparency also opens the parties to charges that there is something to hide and creates vulnerability to sensational revelations such as the reports of a $400 million cash payment to Iran in 2016. Furthermore, it invites the kind of "new discoveries of previously unknown sites" as discussed in the introduction that complicate policy making in the nonproliferation arena and frustrate professional analysts.

Recommendations

1. The P5+1 and Iran should seek opportunities for public ceremonies, press coverage, and diplomatic events to mark important implementation steps.

2. There should also be periodic public and congressional updates on monitoring measures and U.S. support to the IAEA and the Joint Commission.

Key Findings

An important secondary benefit of the Iran nuclear agreement was that it had the potential to be a step toward greater openness in Iran's military and nuclear energy programs, in its politics, and in its relationships with the rest of the world. Iran, however, has not been forthcoming in acknowledging prior and current programs of concern, in establishing additional channels for access between Iran and other countries, and in facilitating further steps toward greater access to the country and to its people. The lack of openness frustrates the ability of companies wishing to do business in Iran to perform due diligence. Such companies cannot be confident about the prospects for long-term trade and the stability of business relationship with Iranian entities. Thus, the lack of Iranian transparency and openness impinges on the very economic benefits that Iran sought in the nuclear agreement.

Recommendation

There should be a priority diplomatic push by members of the P5+1and other interested states, supported by the international business community, toward encouraging Iranian openness and more public release of data concerning implementation and compliance steps by Iran.

Key Findings

The lack of transparency noted above has caused some to question whether the agreement is being fully complied with by Iran. Partisan discord within the United States and diplomatic disagreements between the U.S. and its allies in Israel and the Gulf States about the wisdom of the agreement have worked against shared consensus about the utility of the agreement. Some critics of the accord believe that the P5+1 are insufficiently attentive to monitoring or not serious about pressing for compliance. Even proponents of the agreement worry about Iranian ability to deny and deceive the efforts of monitors and the overall commitment of the Iranian regime to its international promises and assurances. Previous arms control agreements have mitigated such concerns by creating trusted bodies of outside experts to review monitoring efforts at a classified level. Such bodies have built confidence even among skeptics that serious and appropriate monitoring steps were being taken.

Recommendation

A team of outside experts, insulated as much as possible from political pressures, should be created for the Iranian nuclear agreement. Such a team could take one or both of two forms:

- One approach could be to form an independent advisory group of experts to review the monitoring efforts at a classified level. The team, if possible, should issue periodic unclassified summary of its judgments. The team should be composed of a mix of regional Middle Eastern experts, veterans of prior arms control verification efforts, and those savvy in modern technologies and approaches.

- Another approach would be to revitalize the congressional oversight process either through existing committees, a renewed arms control observer group, or through the creation of a Joint Congressional Commission with appropriate bipartisan representation and sufficient expert staff cleared to an appropriate level.[48]

[This page intentionally left blank.]

Section IV – Findings and Recommendations Regarding Technical and Enabling Support to the Nonproliferation NGO Community

Context

Open-source reporting and use of easily available imagery, documents, and media broadcasts (traditional and social) is not a free good. There are risks and consequences for those involved in transmitting and storing this information. Consider this scenario: A citizen or person working in country *X* has acquired information that country *X* might be violating an arms control agreement. This person wants to communicate relevant data to an NGO that serves as a watchdog on potential proliferation activities. If the government of country *X* discovers that this person provided this information to the NGO, the person might undergo harassment, fines, arrest, imprisonment, torture, or execution. Additionally, the safety of that person's loved ones may also be at risk. In recent years NGOs in the international privacy and cyber communications space have been identifying common legal principals designed to shape the state of the law and establish international norms of behavior.[49]

Furthermore, as shown in recent years regarding suspected assassinations by Russian leaders of critics outside of Russia itself, or libel lawsuits in the United Kingdom by suspected members of the A.Q. Kahn proliferation network, the possibility of negative consequences exists for those engaged in reporting of a suspected proliferation target. Beyond the need for suppliers of information to protect themselves, NGOs, governments, intergovernmental entities, and companies involved in the collection, handling, storing, and processing of data must ensure that they are taking all necessary and available actions to protect data that could result in the compromise of someone else' safety, privacy, or liberty. Moreover, nonproliferation NGOs' websites and channels for the communication of their findings are subject to cyberattacks in many forms. If they lose their presence on the web, or the trustworthiness of their websites is compromised, then they lose their ability to influence nonproliferation policy.

Key Findings

Fortunately, encryption protection tools are now openly available to protect people who may wittingly or unwittingly be involved in communicating data related to illicit nuclear activities. To become protected does, however, require knowledge of these tools and an effort to implement them. Moreover, it is important to realize that encryption protection is not perfect, but the tools that are accessible and continually being developed can still help block foreign governmental efforts to censor or persecute individuals and NGOs with sensitive information.[50] The various categories of encryption tools are described below:

- ***End-to-end encryption***: Not all encryption provides the same protection to data along the path from sender to recipient. In general, encryption means encoding data to prevent unauthorized access — in effect, scrambling the data so that it will look like gibberish to a person who views it without decoding using the proper authentication key. End-to-end encryption, in particular, means that the data is scrambled by the sender and stays that way from the path starting with the sender's computer or smartphone and only becoming decoded by the authorized recipient. Thus, this type of encryption protects the data along the entire path from sender to receiver and also

importantly blocks the service provider of the e-mail service, for example, from understanding the data.

- ***Public key cryptography or asymmetric key cryptography***: In the late 1970s, cryptographic researchers began to develop methods to allow encryption and decryption of data using a published public key, which is a very large number and which is paired with a private key, another very large but different "asymmetric" number.[51] Either the public or private key could be used to encode or decode. Both are needed to code and decode the message. Encryption strength increases with key size, and doubling the length of the key would exponentially increase the encryption strength but would decrease the computing performance because of the number of computations needed. But as computing power has increased — typically doubling in size within every two years for a given computer's volume — stronger encryption becomes possible.

- ***Open source encryption technologies***: Open source computer codes, or software applications, are publicly available for computer programmers to read and further develop. From the encryption standpoint, open source codes are usually more reliable because coders and users can verify, "by looking under the hood," that these codes meet the required standards and can work to remove any traps or backdoors that could be exploited by governments or other actors.

- ***Metadata***: The content of a communication is known as data, and information describing the details about the transmission and receipt of that communication is known as metadata, or "data about data." Metadata includes information about where and when the communication was sent, what type of device (laptop or mobile phone, for example) sent the communication, the location of the recipient, as well as the length of time in seconds and the size of the message in bytes of the communication. A communication can be a phone call, email message, or data file transfer over the Internet. While relatively rigorous legal protections are in place in many countries to protect data, such protections are weaker or even nonexistent for metadata.

- ***The Tor Project:***[52] To help protect metadata and to help Internet users obtain anonymity, the Tor Project is a network of volunteer-operated Internet servers that allows users to send information through "a series of virtual tunnels rather than making a direct connection." In addition, the Tor Project's tools can hide information about Web browsing, for example. Moreover, it can help users connect to Websites that are censored by certain governments, and can permit journalists or NGOs to contact people with sensitive information without compromising the identity or whereabouts of those people.

In sum, the above described encryption methods will apply to most if not all of the classic communication channels being used today, including text, voice, instant messaging, file sharing, emails, and cloud storage.

Recommendation

NGOs, in the nonproliferation and nuclear arms control sectors that are collecting, handling, processing, and storing sensitive personal information, should take the necessary actions and use appropriate tools to protect both the information and the physical safety of its providers.

Key Findings

In addition to protecting the safety and privacy of persons, NGOs should also be attentive to the need to protect their servers and public websites from cyberattacks that can compromise, alter, or destroy the very data they have worked so hard to gather. One of the essential missions of many nonproliferation NGOs is to detect and publicize the actions of individuals, businesses, and countries engaged in activities that violate the Nonproliferation Treaty (NPT), United Nations resolutions (such as UNSCR 1540), international laws, or domestic law. While most citizens of most countries would applaud the work of such NGOs, some will not, especially those that are accused of wrong doing and are therefore the subject of enhanced scrutiny. Individuals, businesses, and nation-states are now beginning to react to such scrutiny or accusations. One of the tools to respond to such unwanted scrutiny is cyberattack. Cyberattacks can take the form of a denial of service attacks, spoofing of the NGO's website, redirection of the NGO's traffic to an alternative website, holding the site for a ransom (with either a cash payment and/or retraction demand), or even outright data theft. As part of the Task Force's work, we have discovered that the number of cyberattacks on nonproliferation NGOs has significantly increased over the last year.[53]

Unfortunately, many NGOs' websites are in desperate need of new and better protections from attacks. The problem stems from the fact that many NGO websites are often a kludge of different software and programs, some of which are outdated and no longer supported by the original vendors. This is partly due to the fact that many of the websites were designed with specific funder objectives in mind, with that funding having dried up years ago. The programs may also have been designed by the lowest bidder or by intern volunteers that are no longer updating the sites with software patches. The bottom line is that few of these systems were designed in a comprehensive fashion, thus leaving many unmonitored holes and gaps through which intruders can enter the systems.[54] What is true for these NGOs today, that may not have been the case 10 or 15 years ago, is that the websites have become the crown jewels of the respective organizations. They are the outward presence of NGOs and the collection centers for all of their good work. Many contain valuable data, which are used by others in the nonproliferation community, the loss of which could have significant secondary and tertiary effects.

The concern about cyberattacks should not be limited to NGOs. Governments are also subject to threats but are in a better position, in terms of resources and personnel, to address them.

Recommendation

Funders of nonproliferation NGOs should consider robust funding for upgrades in computer security in order to protect key data, especially if that data is used by other NGOs in the field for their research. The loss of certain databases could be a cascading disaster for the nonproliferation community as a whole. Furthermore, funders should insist that fundees adopt a culture of maintaining good "cyber hygiene" by their personnel as a condition of receiving grants.

ANNEX A

Summary of Recommendations from the Second Task Force Report

1. Ensure that the Joint Commission Works Effectively Among the P5+1 and Iran to Facilitate Compliance and Communication

2. Organize Executive Branch Mechanisms to Create Synergy and Sustain Focus on Implementation Over the Long-Term

3. Support and Augment the IAEA in the Pursuit of its Key Monitoring Role

4. Create a Joint Executive-Congressional Working Group (JECWG) to Facilitate Coordination Across the Legislative and Executive Branches of the USG

5. Prepare a Strategy and Guidebook for Assessing and Addressing Ambiguities and Potential Noncompliance

6. Exploit New Technologies and Open Source Tools for Monitoring a Nuclear Agreement with Iran

Endnotes

[1] "Nonpartisan Nuclear Verification Capabilities Independent Task Force," Federation of American Scientists, accessed September 15, 2017, https://fas.org/nuclear-verification-task-force.
[2] Artificial Intelligence (AI) is usually defined as the science of making computers do things that require intelligence when done by humans. It is an evolving nascent technology. Machine Learning is a sub-set of AI that involves algorithms that can learn to make predictions over time without being explicitly programed to do so.
[3] In this paper, we use the term monitoring to refer to the gathering of information relevant to compliance assessments through intelligence methods, diplomatic means, and negotiated measures such as data declarations and on-site inspections. Verification is the process of reaching political judgments about the extent and significance of compliance and the determination of how to resolve ambiguities or evidence of noncompliance.
[4] Christopher Stubbs and Sidney Drell, "Public Domain Treaty Compliance Verification in the Digital Age*," IEEE Technology and Society Magazine*, Winter 2013.
[5] Chris Ford, Speech at Arms Control Association Annual Meeting, June 2, 2017, accessed August 6, 2017, https://www.c-span.org/video/?429395-4/trump-administration-nuclear-weapons-strategies.
[6] Carol Morello, "Exile group accuses Iran of secret nuclear weapons research," February 25, 2015, accessed July 31, 2017, https://www.washingtonpost.com/world/national-security/exile-group-accuses-iran-of-secret-nuclear-weapons-research/2015/02/24/ad8d64d6-bc5a-11e4-8668-4e7ba8439ca6_story.html?utm_term=.28da6e3537ee.
[7] Statement of Senator Thom Tillis, 114th Congress, *1st Session Issue* 161, no. 69 (2015), May 7, 2015, accessed July 11, 2017, https://www.congress.gov/congressional-record/2015/05/07/senate-section/article/S2727-3.
[8] Frank Pabian, "Commercial Satellite Imagery as an Evolving Open-Source Verification Technology," *Joint Research Technical Reports* (2015), http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97258/reqno_jrc97258_online%20version%20pdf.pdf
[9] Overhead imagery is a broad term designed to include several sensing technologies including photography, video, infrared, lidar, and multi-spectral.

[10] John C. Baker and Kevin M. O'Connell, "Satellite Remote Sensing and Human Rights Monitoring: Implications of Geospatial Affordances of Nongovernmental Organizations" (draft article, June 2, 2017).
[11] "Commercial Satellite Imaging Market (End User – Government, Commercial Enterprises, Civil Engineering Industry, Military, Forest, Agriculture, Energy Sectors, and Insurance; Applications – Energy, Geospatial Technology, Natural Resources Management, Construction and Development, Disaster Response Management, Defense and Intelligence, Conservation and Research, and Media and Entertainment) - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2015 – 2023", Transparency Market Research, 28 February 2016, accessed on September 13, 2017, http://www.transparencymarketresearch.com/commercial-satellite-imaging-market.html.
[12] "Buying Satellite Imagery: Pricing Information for High Resolution Satellite Imagery," LandInfo, accessed on July 3, 2017, http://www.landinfo.com/satellite-imagery-pricing.html.
[13] Google Earth is available at https://www.google.com/earth.
[14] Google Maps is available at https://www.google.com/maps.
[15] Bing Maps is available at https://www.bing.com/maps.
[16] Yandex Maps is available at https://yandex.com/maps.
[17] Here is available at https://wego.here.com.
[18] Baidu is available at http://map.baidu.com.
[19] "Planet Imagery," Planet, accessed on 3 July 2017, https://www.planet.com/products/planet-imagery/.
[20] John C. Baker and Kevin M. O'Connell, "Satellite Remote Sensing and Human Rights Monitoring: Implications of Geospatial Affordances of Nongovernmental Organizations" (draft article, June 2, 2017).
[21] "Pakistan's strategic nuclear and missile industries: A baseline study for non-proliferation efforts – Public version," Project Alpha, September 2016, http://projectalpha.eu/wp-content/uploads/sites/21/2016/11/20160929-Pakistan-public-version.pdf.
[22] Information about Black Sky is available at https://www.blacksky.com.
[23] "Company Info," Facebook Newsroom, accessed August 1, 2017, https://newsroom.fb.com/company-info.
[24] Lucas Matney, "YouTube has 1.5 billion logged-in monthly users watching a ton of mobile video," *The Crunch*, June 22, 2017, https://techcrunch.com/2017/06/22/youtube-has-1-5-billion-logged-in-monthly-users-watching-a-ton-of-mobile-video.
[25] "About Twitter," Twitter, accessed August 1, 2017, https://about.twitter.com/company.
[26] Travis Hunter, "The Social Media Landscape of China – What You Need To Know," *Social Media Authority*, http://socialmedia-authority.com/2016/06/24/the-social-media-landscape-of-china-what-you-need-to-know.
[27] "Momentous Entertainment Group's Chimera Games Unit Launches Its Hit Game on the Russian Social Media Platform VKontakte (VK)," *Marketwired*, July 6, 2017, http://www.marketwired.com/press-release/momentous-entertainment-groups-chimera-games-unit-launches-its-hit-game-on-russian-social-otcbb-mmeg-2225058.htm.
[28] Adrien Henni, "Russia's top 10 websites include Facebook, Google, Instagram, and YouTube," *VentureBeat*, October 1, 2016, https://venturebeat.com/2016/10/01/russias-top-10-websites-include-facebook-google-instagram-and-youtube.
[29] Damien Sharkov, "Ukrainians Join Facebook by the Millions after Russian Social Media Ban," June 20, 2016, http://www.newsweek.com/ukrainians-join-facebook-millions-russian-social-media-ban-627488.
[30] "Active social media users in India grow by 15% from 2015 to become 136 million: Yral Report 2016," *exchange4media*, January 4, 2017, http://www.exchange4media.com/digital/active-social-media-users-in-india-grow-by-15--from-2015-to-become-136-million-yral-report-2016_67225.html.
[31] "Ernst & Young Social Media Marketing," *India Trends Study 2016*, http://www.ey.com/Publication/vwLUAssetsPI/EY-social-media-marketing-india-trends-study-2016/$FILE/EY-social-media-marketing-india-trends-study-2016.pdf.
[32] "Number of TV channels rises by 37 in one year," *Z News*, http://zeenews.india.com/news/india/number-of-tv-channels-rises-by-37-in-one-year_1510793.html.
[33] Mariella Moon, "WhatsApp is becoming a top news source in some countries," *Engadget*, June 25, 2017, https://www.engadget.com/2017/06/25/whatsapp-news-source-reuters-study/.
[34] "Iran profile - media," *BBC News*, May 2, 2017, http://www.bbc.com/news/world-middle-east-14542234.
[35] Phoebe Parke, "How many people use social media in Africa?", *CNN*, http://www.cnn.com/2016/01/13/africa/africa-social-media-consumption/.
[36] See www.Graphika.com

[37] Carole Cadwalladr, "Google, democracy and the truth about internet search," *The Guardian*, December 4, 2016, https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-internet-search-facebook.
[38] Robert G. Parkinson, "Fake news? That's a very old story," *The Washington Post*, November 25, 2016, https://www.washingtonpost.com/opinions/fake-news-thats-a-very-old-story/2016/11/25/c8b1f3d4-b330-11e6-8616-52b15787add0_story.html.
[39] Sabrina Tavernise, "As Fake News Spreads Lies, More Readers Shrug at the Truth," *The New York Times*, December 6, 2016, http://www.nytimes.com/2016/12/06/us/fake-news-partisan-republican-democrat.html.
[40] See generally: David Weinberger, *Too Big to Know* (New York: Basic Books, 2011).
[41] "Posts Tagged: Syria," *Bellingcat*, accessed July 31, 2017, https://www.bellingcat.com/tag/syria.
[42] "Geospatial Technologies and Human Rights," AAAS, accessed on 10 July 2017, https://www.aaas.org/page/geospatial-technologies-and-human-rights-0.
[43] www.geo4nonpro.org
[44] www.38north.com
[45] www.isis-online.org
[46] See https://citizenlab.ca
[47] Valerie Lincy, "The Iran Nuclear Deal: How to Increase Public Transparency," September 14, 2017 http://www.iranwatch.org/our-publications/roundtables/iran-nuclear-deal-how-increase-public-transparency
[48] See the findings and recommendations related to such a Joint Congressional Commission in the Task Force's prior study: "Six Achievable Steps for Implementing an Effective Verification Regime for a Nuclear Agreement with Iran," Federation of American Scientists, August 6, 2015, https://fas.org/wp-content/uploads/2015/08/Six-Achievable-Steps-for-Implementing-an-Effective-Verification-Regime-for-a-Nuclear-Agreement-with-Iran.pdf. Related to this are recent calls by former Senator Sam Nunn and former Secretary of Energy Ernest Moniz, and separately by Robert Kagen, for some form of standing Congressional commission on national security or a revitalized Arms Control Observer Group. See, for example, http://www.nti.org/newsroom/news/new-op-ed-nunn-moniz-urge-formation-liaison-group
[49] Human rights groups have been in the vanguard of development, use, and promotion of encryption protection because of the nature of their work in protecting the identities of persecuted people. See: "International Principles on the Application of Human Rights to Communications Surveillance," Necessary and Proportionate, accessed August 9, 2017, https://necessaryandproportionate.org/principles.
[50] Security-in-a-Box is an NGO that has links to a set of encryption tools and easy-to-understand explanations of how to use them: https://securityinabox.org.
[51] The first published method was developed by Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, November 1976.
[52] Tor Project is available at https://www.torproject.org.
[53] Eric Niler, "DOS Attack Crashes Website Monitoring North Korea's Nuclear Test Site," *Wired*, September 9, 2016, https://www.wired.com/2016/09/dos-attack-crashes-website-monitoring-north-koreas-nuclear-test-site.
[54] Stan Mierzwa and James Scott, "Cybersecurity in Non-Profit and Non-Governmental Organizations," Institute for Critical Infrastructure Technology, February 2017, http://icitech.org/wp-content/uploads/2017/02/ICIT-Brif-Cybersecurity-and-NGOs.pdf.