MITRE | Center for Technology & National Security

INTELLIGENCE AFTER NEXT

RADICAL TRANSPARENCY IN INTELLIGENCE OPERATIONS

by Christian Neubauer

Citizen analysts are revolutionizing intelligence—it's time for the IC to join them…

Over the last decade, news organizations and citizen journalists using new technologies and data sources—including social media posts, commercial satellite imagery, and the digital exhaust of smart phones—have changed the definition of what is possible in uncovering malign activity by nation states and other actors. The powerful capability to observe and expose, previously centralized in state intelligence organizations, is now in the hands of citizens. These efforts change the behavior of global powers using an approach that the Intelligence Community (IC) doesn't normally employ: radical transparency.

The IC has traditionally worked opaquely within secure compartmented information facilities (SCIF) using classified data sources not accessible to the general public. With the rise of publicly available information (PAI) and the democratization of commercial sensor capabilities, the IC risks being outpaced by commercial companies, non-governmental organizations, and other nation-states if it continues to operate only behind closed doors in disconnected environments. Meanwhile, the COVID-19 pandemic is forcing the IC to rethink its approach and the spaces where it works, providing the Community a unique opportunity to reframe its paradigms of classification, intelligence analysis, and information sharing.

The IC can and should move beyond its myopic concern of exposing "sources and methods" and embrace radical transparency to help secure the global community. An open and non-traditional, partner-centric approach to intelligence will improve the scope and impact of the effects the US is able to achieve against malign actors. Radical transparency in intelligence analysis would also be a visible and undeniable step toward collective global security and the rule of international law. The trust it would engender can be a key differentiator between America and other global powers.

THE INTELLIGENCE COMMUNITY SHOULD MOVE BEYOND ITS CONCERN OF EXPOSING "SOURCES AND METHODS" AND EMBRACE RADICAL TRANSPARENCY TO HELP SECURE THE GLOBAL COMMUNITY.

Introduction

In March of 2018, Sergei Skripal, a former Russian officer turned spy for the UK, was having lunch with his daughter at an upscale pub near their home in Salisbury, England. After lunch, the Skripals walked down towards the river Avon and sat on a park bench to talk. An hour later, they were both found unconscious, poisoned with the Russian nerve agent Novichok.

In the months that followed, as the Skripals slowly recovered, the investigative website *Bellingcat* revealed the names and movements of the assassins from the Russian Main Intelligence Directorate (GRU) who poisoned the Skripals [1]. *Bellingcat's* analysis included passport photos, hotel and rental car records, phone records, surveillance footage, satellite imagery, and much more, all published in public forums and accessible to a global audience. What emerged was a damning picture of Russia's willingness to conduct dangerous assassination missions in sovereign nations.

For many within the IC, *Bellingcat's* investigation of the Skipral's poisoning was a wakeup call on the depth and quality of analysis that can be done with purely unclassified sources. Equally as important, the report was a blueprint for how to impact the decision making of other nations against a common adversary. This insight came in the midst of a shift in US thinking

that germinated with the release of the 2017 National Security Strategy which resurrected the phrase great power competition (GPC) to describe the struggle between China, Russia, and the United States on the global stage [2]. Suddenly military commanders, think tanks, and analysts were wondering how to counter the influence of China and Russia in other nations. Bellingcat's approach may be the answer.

The *Bellingcat* investigation is but one example of what is becoming an ever increasing number of similar investigative reports published by news organizations and citizen journalists around the world within the last decade.

- *The Washington Post* tracked and exposed the Israeli operatives that assassinated Mahmoud Al-Mabhouh in the United Arab Emirates in 2010 [3] and the Saudi Arabian team that killed Jamal Khashoggi in Turkey in 2018 [4].
- *Bellingcat* itself identified the Russian operatives who assassinated Zelimkhan Khangoshvili at a beer garden in Berlin in September 2019 [5] and, with *Der Speigel* and *The Insider*, identified the team that poisoned Alexander Navalny in Novosibirsk in August 2020 [6].
- A joint investigative team led by the Dutch Ministry of Justice tracked the Russian surface to air missile system and military technicians that shot down Malaysian Airlines flight 17 over the Ukraine in 2014 [7].

These investigations have led to indictments, arrests, financial asset forfeitures, expelled diplomats, and international condemnation [8] [9]. The Skipral investigation resulted in 28 countries expelling 150 Russian diplomats and intelligence agents. These efforts changed the behavior of nation-states by directly naming malign actors [10]. That effect was achieved by radical transparency.

Democratized Intelligence Analysis

The common thread across these efforts is the power of modern technology to democratize investigation. New technologies and data sources from traffic cameras to smart phone geolocational data put investigative capabilities in the hands of the citizenry. Organizations as diverse as financial institutions, humanitarian groups, and sports teams employ data analysts to gain a competitive advantage or understand their operating environment. Nations across Africa, Asia, and South America can track visitors using sophisticated biometrics gathered at entry control points. They can conduct robust forensic analysis using public street cameras to understand criminal activities within their borders. They can track license plates and cell phone activity and see malign actors moving from airports to hotels. Citizen groups can track planes using amateur radar. They can set up cheap sensors in their back yards to listen for gunshots. They can look for deforestation or illegal mining activities in satellite imagery. The powers to observe and expose that used to be centralized in major state intelligence organizations are now in the hands of small nation-states, companies, and citizens.

The increasing ubiquity and ease of use of artificial intelligence (AI) and machine learning (ML) means that attempts to "hide in plain sight" are increasingly untenable. Commercial companies are creating constellations of satellites looking at all areas of the globe. ML can parse through that satellite data to find ships on the ocean anywhere on the planet. ML can also watch construction activities, look for mass graves, and track deforestation [11]. As commercial companies launch more capable satellites with real time video feeds beamed back to earth at a relatively low cost, there will not be a spot on the globe that can't be seen and analyzed. Similarly, the ubiquity of smart phones, everyone a bundle of powerful sensors that record, track, and measure the world around them, means we

are all in some sense connected to the global network.

How do we consolidate these grassroots efforts to inoculate global society against malign actors in support of U.S. national interests? There are existing models that bring together coalitions of global organizations to promote our collective security against state actors and international criminal organizations. MITRE ATT&CK®, for example, is a repository of global knowledge describing how cyber adversaries infiltrate and exploit computer systems [12]. ATT&CK is updated and maintained by a coalition of international participants and forms a common global awareness of how attackers operate. Critically, the knowledge stored in the system, referred to as Tactics, Techniques, and Procedures (TTPs), feeds automated intrusion detection software run by companies that operate on the internet. This software can use those TTPs in conjunction with sophisticated artificial intelligence to establish patterns of activity and shut down attacks before they happen [13].

The global coalition of law-abiding nations needs a similar international effort to track and document the TTPs of malign actors in the physical space. This shared understanding of how malign actors operate and how they avoid detection will deny them freedom of movement and deter future attacks. Most importantly, we must do this transparently, in a public space, and with partner nations to offset the disinformation campaigns that inevitably accompany public identification of malign actors and their activities. The collective TTPs of malign actors can feed the physical equivalent of cyber intrusion detection systems: the ubiquitous public camera systems embedded in smart cities, the biometrics systems that govern airports and border crossings, and the commercial sensors technologies that track the movement of equipment and people around the world. As these systems become more sophisticated and are connected to law enforcement agencies, malign actors can be deterred, countered, or even caught the minute they step off the plane or drive across the border.

A New Paradigm for the IC

The IC collects and uses much of the same information as investigative organizations and citizen journalists to expose malign actors. It has specialized in and honed the analysis of public data to draw conclusions under the aegis of "open-source intelligence", or OSINT. Using publicly available information as well as geospatial intelligence (GEOINT), electronic intelligence (ELINT) and other techniques, the IC conducts similar investigations into malign actors to inform decision makers on how to direct the instruments of national power against this threat.

Unlike their public counterparts, the IC traditionally performs these functions in a classified environment to protect 'sources and methods'. The IC combines unclassified datasets with classified data to draw conclusions, theoretically giving the IC a leg up on citizen journalists. The IC's efforts have a serious downside though, as they are opaque to the global community. The inclusion of classified sources in the IC's analysis makes their conclusions difficult or impossible to share with the public, with law enforcement agencies, or in some cases even with like-minded partner nations.

The IC is traditionally unwilling to share sources and methods under the premise that letting malign actors know how you find them will help them hide more effectively. This premise falters under the paradigm of democratized intelligence, where the bad actors are just as savvy and capable of using the same data and analytic techniques as the IC. It also ignores the GPC necessities of swaying decision makers in partner nations and global public opinion against our adversaries with transparent evidence of wrongdoing.

Global corporations operating in the democratized landscape of the internet were confronted with the same challenge from hackers, thieves, and criminal syndicates years ago and came to the conclusion that radical transparency increases the effectiveness

of our collective defense. Virus scanning companies openly publish and share rule sets. Companies like Microsoft, Google, Twitter, and Facebook publish detailed descriptions of attacks and mitigation strategies [14]. Companies share attack TTPs with their own competitors because they understand the value of collective security that that transparency brings.

We are at an inflection point with public and commercial sensing technologies. Soon there will be no hiding in the physical world from ubiquitous global surveillance– some may argue that we are already there. Information on specific crimes break almost immediately on public platforms such as Twitter and YouTube.

Coalition building and leadership on shared security is a role where the U.S. can excel. As nations like China and Russia increasingly pursue their own interests on a global scale, the United States can serve as a counterbalance [15]. Radical transparency in intelligence analysis would be a visible and undeniable step towards collective global security and the rule of international law. The trust it would engender can be a key differentiator between America and these autocratic regimes.

Embracing Radical Transparency

The IC has experimented with radical transparency in the past. The CIA began publishing its World Factbook publicly in the 1970s. In the last few years, forward-thinking leadership at the National Geospatial-Intelligence Agency (NGA) established the tearline.mil website to publish intelligence in public spaces and to create shared dialogue around analytic techniques [16]. COVID-19 can be the catalyst for the IC to pursue radical transparency broadly. As analysts are forced to adapt to working more effectively outside the office, the IC has expanded its ability to share and disseminate information [17]. The slow shift away from exquisite, classified sources of intelligence and toward publicly available information is becoming an urgent necessity. How do we take advantage of this shift? Investigative

THE IC SHOULD ESTABLISH AND DRIVE A PUBLIC REPOSITORY OF KNOWLEDGE TO DETECT AND TRACK COVERT ACTORS.

organizations and citizen's groups like *Bellingcat* publish guides to teach citizens to dive into investigation via sources like social media or flight tracking data [18]. There are numerous amateur groups that explain how to conduct hunts via satellite imagery [19]. Humanitarian organizations publish data sets and real world examples of data visualizations that help expose corruption and malfeasance [20]. The IC should embrace these movements as full partners in the effort to secure the globe, learning from their efforts and sharing knowledge back on methods and techniques as NGA has done with tearline.mil. The IC should fund and incentivize these organizations through programs like the Intelligence Advanced Research Projects Activity (IARPA). Imagine a nation of citizen investigators on vigilant alert, with the tools and knowledge to wade through disinformation and find evidence they need to prevent the next attack on our collective global security.

The IC should also establish and drive a public repository of knowledge to detect and track covert actors. This repository should document the TTPs used by covert actors to hide, conceal, and dupe and the mechanisms that can be used to expose those actors. Each underlying TTP should be linked back to real world observations of malign activities. Critically, the repository should contain mitigation strategies to help defeat these TTPs. As gaps are discovered in the global security apparatus at points of entry into countries and in international sharing systems, the United States should fund partner nations to close holes and address gaps. Where TTPs are found to be useful in detecting malign actors, they should be included in security procedures at tourist vetting locations and in visa processing.

In the same way that we help other nations protect the integrity of their election systems, fight piracy, and establish rules based legal systems, we should work to help them protect their borders and citizens from malign actors.

The TTP repository should be established in partnership with other nations, non-governmental organizations, and citizen groups to maximize the dissemination of information and to allow data sets and analytic methods from this community to flow back into the IC. Participation by other nations can be encouraged through multilateral and bilateral agreements. This forum should be the primary dissemination mechanism for intelligence that can lead to deterrence or conviction of malign actors by, with, and through our partners.

The IC will continue to operate on classified networks with classified sources but needs to dramatically rethink the balance between what is done in classified spaces and what can be done in public. The IC needs to reconsider classified sources and methods and acknowledge that sources and methods used broadly in the public domain should not be classified in the IC. This shift of data, tradecraft, and staff to public spaces will require significant effort by policy makers to ensure that the rules for sharing information and operating on unclassified networks are in place. Again, NGA has led the way here and can provide a pathway for the rest of the IC.

Importantly, we need to embed measures of authority and validity in our shared intelligence processes. Everything from news reports, to audio recordings, to videos can be faked with the help of machine learning tools available broadly on the internet [21]. In the past, these sorts of deception activities were easy to expose but with the rise of generative artificial intelligence and deep fakes, it is more difficult to uncover the truth. Without a clear understanding of the motivations of news outlets, the potential for fakery in a given technology, or even the biases built into human decision making, we will be challenged to draw accurate conclusions. Fortunately, the IC's deep experience in understanding denial, deception, and disinformation can be shared to establish authority and validity in our collective consciousness through this repository.

Conclusion

The Skripals survived the attack in 2018. After being released from the hospital, they were put into protective custody. Other targets of international assassination were not as fortunate. Assassins killed Alexander Litvinenko in London in 2006 and Kim Jong-nam in Kuala Lumpur in 2017. The families of the 298 passengers killed on flight MH-17 have yet to see anyone brought to justice. We must work to arm law-abiding nations with the tools they need to protect themselves from future attacks and to change the behavior of malign actors acting with the active support of nation-states that would do us harm.

Ultimately, the convergence of technology and connectivity will lead to ubiquitous surveillance. Legislation and ethical debate will not protect us from this reality. We can wait for these changes to come and irreversibly alter the way America conducts intelligence and military operations, or we can use this revolutionary change in the pursuit of global values and human rights. In doing so, we can fight against authoritarian regimes, enhance U.S. national security and build a global society that comes with a built-in democratic immune system. The IC has an opportunity to lead the way.

References

[1] *Bellingcat*, "Bellingcat–Skipral," Nov. 25, 2020. [Online]. Available: https://www.bellingcat.com/tag/skripal/

[2] U. Friedman, "The Atlantic," Aug 6, 2019. [Online]. Available: https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/

[3] *The Washington Post*, "Fake passports fuel questions about Israeli role in Hamas official's slaying," Feb. 17, 2010. [Online]. Available: https://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021700544.html?hpid=moreheadlines

[4] Reuters, "How the man behind Khashoggi murder ran the killing via Skype," Oct. 23, 2018. [Online]. Available: https://www.reuters.com/article/us-saudi-khashoggi-adviser-insight/how-the-man-behind-khashoggi-murder-ran-the-killing-via-skype-idUSKCN1MW2HA

[5] *Bellingcat*, ""V" For "Vympel": FSB's Secretive Department "V" Behind Assassination Of Georgian Asylum Seeker In Germany," Feb. 17, 2020. [Online]. Available: https://www.bellingcat.com/news/uk-and-europe/2020/02/17/v-like-vympel-fsbs-secretive-department-v-behind-assassination-of-zelimkhan-khangoshvili/

[6] *Bellingcat*, "Hunting the Hunters: How We Identified Navalny's FSB Stalkers," Dec. 14, 2020. [Online]. Available: https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology/

[7] Dutch Safety Board, "Crash of Malaysia Airlines Flight MH17," Nov. 2015. [Online]. Available: https://www.onderzoeksraad.nl/en/media/attachment/2018/7/10/debcd724fe7breport_mh17_crash.pdf

[8] US DOJ, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," Nov. 4, 2018. [Online]. Available: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

[9] P. Wilson, "Voltaire Network," Oct. 4, 2018. [Online]. Available: https://www.voltairenet.org/article203340.html

[10] J. Landsdale, "Transparency–The tool to counter Russia," BBC, 2018. [Online]. Available: https://www.bbc.com/news/uk-45751173. [Accessed 15 12 2020]

[11] Citizen Evidence, "Where to Access Satellite Imagery," March 20, 2020. [Online]. Available: https://citizenevidence.org/2020/03/20/magery/

References

[12] MITRE, "MITRE ATT&CK," Nov. 25, 2020. [Online]. Available: https://attack.mitre.org/

[13] B. e. a. Strom, "Finding Cyber Threats with ATT&CK Based Analytics," MITRE, Annapolis Junction, 2017.

[14] FireEye, "Double Dragon: APT41, a dual espionage and cyber crime operation," 2019. [Online]. Available: https://content.fireeye.com/apt-41/rpt-apt41/

[15] USAFRICOM, "Posture Statement to Congress 2020," 2020. [Online]. Available: https://www.africom.mil/document/32925/2020-posture-statement-to-congress

[16] NGA, "Tearline.mil," NGA, Dec. 2020. [Online]. Available: https://www.tearline.mil/about-tearline/

[17] K. Linnebur, C. Callsen, M. Stromecki and C. Hedrick, "INTELLIGENCE AFTER NEXT: THE FUTURE OF THE IC WORKPLACE," Nov. 2020. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-20-1891-intelligence-after-next-the-future-of-the-ic-workplace.pdf

[18] Bellingcat, "Guides," Nov. 25, 2020. [Online]. Available: https://www.bellingcat.com/category/resources/how-tos/

[19] Exposing the Invisible, "Starting Satellite Investigations," July 31, 2020. [Online]. Available: https://exposingtheinvisible.org/en/guides/starting-satellite-investigations/

[20] openAFRICA, "openAfrica," 2020. [Online]. Available: https://africaopendata.org/about. [Accessed Dec. 24, 2020].

[21] Bloomberg Quicktake, "It's Getting Harder to Spot a Deep Fake Video," 2018. [Online]. Available: https://www.youtube.com/watch?v=gLoI9hAX9dw

Author

Christian Neubauer is the Chief Engineer for European Operations at MITRE. He has worked across Intelligence Community agencies and within the combatant commands at the intersection of intelligence analysis and technology innovation.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's analytical workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the IC's analytical community in the post-COVID-19 world.

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | Center for Technology & National Security