ISN
ETH Zurich

21 July 2015

Open Source Indicators and Asymmetric Advantage in Security Planning

Can the West use its unfettered access to open source information to maintain its asymmetric advantage in security planning? Regina Joseph believes so. However, there are problems that have to be faced, including the authenticity of the information that's available and its sheer size.

By Regina Joseph for ISN

Imagine the following global conditions: after several years of exhausting conflict, a propaganda battle ratchets upwards in an attempt to spread the influence of new political movements, mobilize masses and attract members to causes via new media outlets. On one side lie the political and business elites, who control and/or own most information channels. On the other lie smaller niche groups, some of whom have extremist ideologies. The elites fear radical subversion, especially as they watch these groups nimbly circumvent a lack of access to information channels by successfully reaching people through more direct means. That success is driven by a grinding " psychological and cultural isolation" and "loss of security faced by citizens once bound and sustained by informal social rules and orders", a development that has rendered people uniquely receptive to anti-democratic and nihilist rhetoric.

If that sounds like a description of today's headlines regarding the so-called Islamic State and neo-fascist right-wing groups, you would only be half-right. The scenario above describes the post-World War I battles for hearts and minds by Communist, Socialist and Fascist groups who used then-emerging conduits like radio to attract war-weary citizens. Media was as forceful a tool for engineering human behavior then—a time when propaganda theory was in its ascendance—as it is now.

Today, the Internet also acts as a force multiplier for media, creating new dissemination channels by tearing down entry barriers for public communication and distribution—whether via social media, blogs or YouTube. For many Western countries, this digital firehose of free speech is perceived as a manifestation and natural extension of the democratic identity. For other states, it is a force to be both feared and used, whether as a tool to control their own societies or as a weapon to manipulate others. Russia's troll factories and China's 50-Cent Party of hired "public opinion guides" represent some of the more notorious attempts to keep people pliant and to bend narratives in service of state objectives.

With so much more information now cheaply and easily available to anyone with uncensored Internet

access, a strategic security domain is emerging. Whereas the business of defense has always been predicated on privileged and classified information meant for the eyes of a highly select few, new research initiatives that merge human cognitive judgment, machine learning and artificial intelligence (AI) suggest that open source information can—in certain cases—be as (if not more) tractable when trying to predict economic and political events. Yet, while such findings may elicit conclusive security advantages in the future for states that uphold free speech, authenticity and volume pose greater near-term difficulties to be overcome.

The Good News…

Since the development of the Internet in the late 1960s, the Defense Advanced Research Projects Agency (DARPA) and other agencies have sought to harness its national security potential. For instance, the Internet's facilitation of data collection has enhanced research once dependent on onerous data scraping from analog sources. AI, machine learning and natural language processing (NLP) techniques designed for trawling the net's vast resources have opened up new vistas in anticipatory intelligence. In this respect, the Intelligence Advanced Research Projects Activity's (IARPA) Office of Anticipating Surprise (OAS) is one of the leading repositories of programs dedicated to testing the potential of predictive analytics to enhance strategic security. These include the Aggregative Contingent Estimation (ACE) Program and other open source projects like the handily-titled Open Source Indicators (OSI) program.

OSI aims "to develop methods for continuous automated analysis of publically available data in order to anticipate and/or detect significant societal events, such as political crises, mass violence, riots, mass migrations, disease outbreaks". The program's top performer was a forecasting model put together by researchers from Virginia Tech, Raytheon and Hughes Research Laboratories called EMBERS (Early Model Based Event Recognition using Surrogates). By sifting through more than 200,000 blogs, Twitter's entire feed pipeline, and satellite imagery, EMBERS produced alerts that accurately predicted events of civil unrest—although it is still improving upon getting all the particulars of the predicted events correct.

Whether generated by humans or software agents, accurate forecasts derived from publically available media sources represent a distinct advantage in strategic foresight. Aside from the value of the forecasts themselves, the potential cost-benefit ratio—especially compared to that of classified information during a time of budget cuts and sequestration—requires serious consideration. A critical caveat, however, lies in the rapidly multiplying costs of open source media.

…And the Bad

Two major challenges in using open source media lie in its verifiability and the total volume available. Starting with the latter, the sheer numbers are staggering. In 2012, 2.5 exabytes of data were created every day, a number calculated to double approximately every 40 months. And while data is becoming cheaper as it becomes more ubiquitous, the cost of managing it is on the rise. Data science is a relatively new profession, and is thus professionally underpopulated. That scarcity exacerbates the problems caused by the mismatch between data containing 'signal' and data containing 'noise', which rises in direct proportion to the total amount of new data generated every second. While new software programs and system architecture emerge to separate the wheat from the chaff, researchers estimate that 30% of key data goes unused because of the difficulty involved in physically accessing it.

While this poses tactical complexity and economic burden, the real risk in using open source media lies in a burgeoning information arms race. Fake news and disinformation can be created and spread as easily as real and objectively reported news. Distinguishing between the two has become

increasingly tough. In authoritarian states where Internet use is carefully monitored (if not censored outright), government-led units designed to flood the Internet with faux Twitter feeds, Photoshop-doctored images, and phony news items are common. Peter Pomerantsev has chronicled Russia's "weaponization of information" and the role it has played not only in sowing confusion among citizens in Ukraine and the Baltics, but also abroad, where foreign analysts and reporters must go to great lengths to understand what is real and what is false in the country's reporting.

But disinformation and propaganda are only part of the problem. Declining revenues in the media world mean fewer professional journalists, thus augmenting the potential for incomplete information. That can take the shape of news aggregators sloppily copying or cutting and pasting information on a second- or third-hand basis, or it can appear in the form of young, cheap hacks who lack sufficient knowledge and experience to convey important nuances (or who fabricate altogether). At the business level, media convergence and consolidation concentrates information outlets under the control of only a handful of corporations or singular owners (such as Rupert Murdoch or Silvio Berlusconi) who often struggle with editorial objectivity and curation, especially if it flies in the face of profits.

In the cybersecurity realm, the problem of information deception has been a longstanding concern. For instance, Dartmouth College computer science professor and researcher Paul Thompson has written extensively on the effect of cognitive hacking on computer systems. Thompson has called for the development of a "News Verifier" program that can prevent attacks on a digital network by allowing administrators to check possible misinformation before it compromises a system. Indeed, given the possible security advantages offered by foresight initiatives like the Good Judgment Project or EMBERS, a "news verifier" tool could become as vital for human forecasters and software models working the geopolitical realm as it is for computer scientists. Moreover, if tools for filtering, aggregation and fact-checking can be developed to hone the potential for predictive analytics, it's worth considering how this might fit into a larger security and defense planning scheme.

A Possible Opportunity?

When former US Secretary of Defense Chuck Hagel called in late 2014 for innovative approaches to counter a perceived loss of technical advantage during a time of austerity, he evoked two historical antecedents. By proclaiming a need for "a game-changing offset strategy," Hagel referenced the Offset Strategy created in the 1970s under then-Secretary of Defense Harold Brown. Devised against the backdrop of economic restrictions imposed after the Vietnam War, it sought to maintain a superior defensive advantage through new microelectronics, stealth and information technologies. However, the central driver behind the strategy was to asymmetrically offset the quantitative edge achieved by the Soviet Union after it reached nuclear parity with the US. This so-called "offset" took its cues from the precursor "New Look" strategy devised in the 1950s under President Dwight Eisenhower. New Look's offset was built on the superior technical advantage the US had at that time in its nuclear arsenal and missile delivery systems.

In a 2014 report for the Center for Strategic and Budgetary Assessments, Robert Martinage suggests the development of a third offset strategy, one built on targeting the anti-access/area denial (A2/AD) advantages held by other states. This would consist of a Global Surveillance and Strike (GSS) Concept which leverages the "US' 'core competencies' in unmanned systems, automation, extended-range and low-observable air operations, undersea warfare and complex system engineering and integration." In short, drones, robots, lasers, and undersea payload technologies combine to offset the advantage other countries now have with A2/AD.

This and other offset strategies proposed elsewhere remain heavily rooted in the battlefield-based/theatre of operation concept of warfare. Yet, as conflicts become increasingly

transnational, unconventional and virtual (as in the case of zero-day cyberattacks), such offsets—predicated on current US technical and economic comparative advantages—may confer very little asymmetry. As automation and unmanned vehicle technologies proliferate across the globe, US asymmetric advantages in those areas may not last for long.

However, one overlooked asymmetric advantage the US and many of its Western allies do hold is the uncensored access to information and knowledge they grant their citizens—the exploitation of which has been a significant factor not only in US digital dominance (Google, Apple, Facebook and Amazon are some of the world's largest companies by market capitalization) but also in the progress of OSI-based anticipatory intelligence programs like the ones run by IARPA and DARPA. Resiliency and innovation are by-products of societies which uphold free speech; the strengths of societies permitted to roam the Internet stands in contrast to the dependencies of countries that dictate their inhabitants' understanding of the world.

Possible Ways Forward

Strategic foresight security programs designed to anticipate geopolitical outcomes could serve as one facet of a truly asymmetric offset strategy. Martinage notes the US' comparative advantage in AI, NLP and machine learning—all of which form critical parts of any strategic foresight platform. Clearly, the issues of verifiability and authenticity would need to be addressed. Additionally, an OSI-based program would likely confront the generational, economic and dispositional aspects of a military-defense industrial complex still built primarily upon machinery rather than human capital. These factors would be a challenge to mitigate—but not impossible

Further research will drive the leading edge on how humans can harness the universe of information at their fingertips. It will also examine how technology can assist humans to glean insights that may provide asymmetric security advantages. Whether these will be taken up as part of a new security approach, however, remains to be seen.

For more information on issues and events that shape our world, please visit the ISN Blog or browse our resources.

Regina Joseph is the founder of Sibylink, an international consultancy based in The Hague and New York devoted to providing strategic foresight on global issues through futures forecasting and analytical training. A Good Judgment Superforecaster, she is also the co-founder of Super-Powered, which produces analytical media. She is also a faculty member at New York University's Center for Global Affairs, where she will be launching a Futures Lab in Fall 2015.

Her website can be found at http://www.sibylink.com; http://www.super-powered.com; Super-Powered on YouTube Super-Powered THE SHOW!; LinkedIn https://www.linkedin.com/pub/regina-joseph/1/b21/780; Twitter: @Superforecastr;

Publisher

International Relations and Security Network (ISN)