Influence Operations and the Intelligence/Policy Challenges

Greg Treverton

CATS
Center for Asymmetric Threat Studies

Swedish Defence University

Influence Operations and the Intelligence/Policy Challenges

CATS Conference 4–5 May, 2017

Author: Greg Treverton

Preface

Recent events in the West concerning the role of influence operations within a greater security policy context and directly in the election processes have reminded us of lessons how we handled the phenomena that was labelled "active measures" during the Cold War period. The central question is what kind of new relationships and inter-government cooperation must be developed in response to these influence operations. Against this background this conference note is based on a workshop which took place in Stockholm between 4-5 May 2017 on the role and upcoming challenges for the Intelligence Communities.

Dr. Greg Treverton
Former Chair of the US National intelligence Council (NIC) and senior fellow with CATS – has edited these proceedings from this highly appreciated event and timely subject.

Dr. Lars Nicander
Director, Center for Asymmetric Threat Studies (CATS)

Title: Influence Operations and the Intelligence/Policy Challenges

Author: Greg Treverton
Center for Asymmetric Threat Studies (CATS), Swedish Defence University

ISBN: 978-91-86137-66-3

The report can be downloaded from www.fhs.se

Influence Operations and the Intelligence/Policy Challenges

This conference aimed to assess influence operations, especially those conducted by Russia, in the context of changing relations between intelligence and policy and the emerging challenges for intelligence. With regard to influence operations, the challenge is to:

- "Identify" (How do we separate state sponsored disinformation from stupidity)
- "Understand" (How do we understand Influence Operations and how do we put it into a context for senior policy makers and how can we learn to understand the underlying factors and why it happens)
- "Counter" (how should we vaccinate our civil servants (including the need for disseminating threat information) and enhance the critical approach within media.)

Session 1: Identifying and Understanding Influence Operations in the Context of Policy

Challenges for Intelligence in the Context of Intelligence-Policy Relations. The conference was conducted under Chatham House rules, but this framing session began with my reflections on my recent tenure as chair of the U.S. National Intelligence Council (NIC). It focused mostly on intelligence and its connection to policy to frame some of the challenges facing intelligence in the future. It did discuss the latest episode of "influence" operations – the Russian hack into the emails of the Democratic National Committee (DNC) and accompanying issues. Its conclusion is reflections on a distinctly "non-normal" time ushered in by the election of Donald Trump as U.S. President.

- *National Intelligence Council (NIC).* The NIC is the arm of the U.S. director of national intelligence (DNI) for Inter-agency analysis. That is, if the president or another senior official wants the CIA view of an issue, he or she can ask the CIA. Most of the time, though, officials want to know what the "Intelligence Community" thinks. That, then, falls to the NIC, with 100 analysts, organized like the State Department with National Intelligence Officers (NIOs) for

regions and functions. They will convene "their" community of analysts from the various agencies, and decide on the answer and how to produce it. The people are terrific. The good news is that intelligence in general and the NIC in particular are very embedded in the policy process. That probably is mostly a consequence of the fact that the United States has been fighting wars for the last generation since 9/11. Now, the NIC is the primary intelligence support for the two main policy committees in the U.S. government – the Principals Committee (the relevant cabinet secretaries in foreign affairs) and the Deputies Committee (their deputies, who assess options and tee up decisions for the principals).

- *Balancing Strategic and Tactical.* This is an enduring challenge; hand-wringing about the primacy of the urgent over the important has characterized all of my years as a student, consumer and sometime practitioner of intelligence. Historically, the NIC had been mostly strategic. The strategic challenge is made worse by the shapelessness of the current world, which means that every crisis has to be approached afresh on its own terms, and, especially, by the nation's hyper-sensitivity to the terrorism threat. That threat to the United States homeland remains minimal, but that is hardly the way it is perceived by the public – or characterized by politicians. From my perch at the NIC, the acute sensitivity was doubly deforming of our work. When we looked at Nigeria, there was not much Nigeria: it was Boko Haram. And even when we looked at Boko Haram, there was not much Boko Haram: it was all deciphering networks and targeting bad guys. We all wondered and worried, where do these people come from, and why are they doing what they're doing? We did what we could at the NIC trying to understand root causes and motivations. But we were only scratching the surface.

In 2016 the NIC produced about 700 pieces of paper, and more than half of those were memorandums from a National Intelligence Officer to the National Security Adviser, her deputy or another senior National Security Council official. They came directly from the deliberations of the Principals Committee or, especially, the Deputies Committee. Not all those were purely tactical. Some were the "what ifs?" of the sort that should be the woof and warp of intelligence-policy relations: "if we do x, how will Putin respond?" Because we were at all the policy meetings, we knew what was going on. But my task, every day,

was to find time and capacity not just to answer the questions policy officials asked but also to answer the more strategic ones they weren't asking.

- *Building – and Adjusting – "Stories" in a Shapeless Word.* This is a kin of the strategic/tactical challenge, and one that bears more directly on warning. I have come to think that intelligence is ultimately about telling stories, and most "intelligence – or warning – failures derive from holding onto stories that events have outmoded. A story from another realm, ebola, drives the point home. The medical community had a "story" about ebola: because death was quick, its period of contagion was brief, thus it would flare up and die out in remote regions. Trouble was that much better transit from rural areas to urban had overtaken the story.

The shapelessness of the world both confounds and demands strategic analysis. If intelligence is story-telling, many of our current stories are suspiciously long in the tooth. In policy terms, for instance, we have been telling ourselves the same story about North Korea for a generation: with just the right combination of carrots and sticks, primarily the latter, and with China as a real partner, we can induce North Korea to foreswear nuclear weapons. Meanwhile, North Korea has gone from an incipient nuclear power to a real one. Intelligence cannot prove and thus cannot say the truth: North Korea is a nuclear power and will remain one; that is all the regime has. But at least challenging the prevailing story would be a start.

For other critical issues, like the Middle East, we have no real story beyond demonizing terrorists and Iran. To be sure, the task is hard. Throughout my tenure at the NIC, I looked for strategic insights and found precious few because the issues are complicated and the causal arrows tangled. The best I found came from our Australian colleagues, who divided the conflicts into three and a half factions – the ISIL-led Sunni extremists: the Saudi-led Sunni autocrats; the Iran-led Shi'ias; and the missing half, the Muslim Brotherhood-led Sunni moderates, recognizing that the term "moderate" is relative at best. But the difficulty of the task is no justification for not trying it. Otherwise, we can all too easily blunder into major campaigns against minor threats or still worse, create those threats.

- *Transparency and "Big Data."* These are two sides of the same coin. The same ubiquity of information that produces so much for intelligence agencies to assess also makes it impossible for their operatives to remain secret for long – and, alas, guarantees that there will be more leaks of methods if not more Snowdens. Perhaps

> the vision of the future should be more akin to Silicon Valley where secrets are kept but not for long and where the premium is on collaboration even if today's partner may be tomorrow's competitor.

But that data will be a godsend for intelligence. To be sure, the analytic challenge is greater for intelligence than for private businesses, most of which wants to predict where I will be tomorrow so they can besiege me with ads for things I like. At the NIC, I started an experiment in the Africa account. Its premise was that while there isn't a huge amount of intelligence information on Africa, there is a lot of data out there; the goal was an existence theorem: if the NIC, with a hundred analysts, could make use of data, any place in the Intelligence Community could. Not surprisingly, we found that social media and other available data was pretty good at predicting famine and disease. The next step was to cull "tips" from the data: where should analysts look, what connections should they probe that they hadn't considered.

The NIC also inherited a nifty bid of crowd-sourcing that had been developed by IARPA, intelligence's counterpart to DARPA, the Intelligence Advanced Research Projects Activity. There were two prediction markets, one classified and composed on intelligence professionals and the other unclassified. The open one was the creation of Philip Tetlock, and it had made two important discoveries. Just as some people are better athletes than others, so, too, some people are better predictors; his open market came to feature "super-predictors." Even better, a small amount of training improves prediction. Unsurprisingly, the burden of that training is helping people keep an open mind just a few seconds longer. I used the internal market as a kind of "red cell": if the experts thought development x was y percent likely but the market was betting 2y, what was going on? I didn't care about the numbers, it was the conversation that mattered. And I hoped to move to market from fairly short-run predictions, which could be settled soon, to longer, more strategic questions. For them, I hoped we might create way-stations on which to bet and, in the process, perhaps do better at constructing what intelligence calls "indicators."

- *Breaking the Cycle.* It has been long and often said that the canonical intelligence cycle, from requirements through collection to analysis and dissemination, is often short-circuited. That is true enough – no matter how much intelligence agencies dislike it, policy officials will hanker for the next "raw" spy report or intercept. But as a paradigm the cycle is increasingly unhelpful. In this as in many other ways, what worked tolerably well in the Cold War is dysfunctional now. Then, with one over-arching and secretive foe, it made a certain sense to ask, in a linear way, what we needed

to know and how we might collect it. Even analysis had a certain industrial quality about it: a fried who was an NSA Soviet analyst recalls starting the day with a large stack of "her take," the overnight SIGINT collection relevant to her account.

Before I returned to the NIC, I had become a fan of "activity-based intelligence," or ABI. It was developed in the war zones in Afghanistan and Iraq primarily to unravel terrorist networks and identify bad guys. Identifying Osama bin Laden's driver was one of its successes. It amassed information from many sources around particular locations, then used correlations to develop "patterns of life" that would distinguish potential terrorists from ordinary pious Muslim at pray. For me, its side-benefit was creatively disrupting the canonical cycle. It was "sequence neutral": we might find the answer before we framed the question. Think how often in life that occurs; you don't know you were puzzled about something until you find the answer. And in a world of ubiquitous information, ABI doesn't prize secret sources: if information is useful, it's good; if not, not. Finally, perhaps advancing age has made be skeptical of the causation that infuses the canonical cycle. I feel more comfortable with correlation while recognizing that many of the correlations will be spurious.

- *Intelligence as an Argument for Policy.* This, too, is hardly new. In the past, in times of divided government, Congress was tempted to, in effect, turn intelligence issues into policy choices by mandating that if intelligence caught Iran exporting x, then y sanctions would be automatic. To be sure, the practice was more than uncomfortable for intelligence, for it meant asking intelligence to put a gun to the heads of its policy counterparts in an administration! More recently, it days of intense partisanship, administrations have been tempted to use intelligence to argue for their policy choices. So it was in the run-up to the 2003 invasion of Iraq. The intelligence assessment that Iraq had weapons of mass destruction made it difficult for Democrats in Congress to oppose the invasion and provided policy cover for supporting it. So, future administration will be tempted to turn intelligence findings into policy choices: imagine if the Community found what is so far has not – evidence that Iran was persistently cheating on its obligations under the nuclear deal.

- *New Competitors, New Colleagues.* Intelligence has always worried about the competition. A generation ago that was CNN: was intelligence always to be scooped by CNN? (I always thought that concern was misplaced: better to get it right than get it wrong,

first.) Now, though, the list of sophisticated private organizations doing "intelligence" is a long one, from Eurasia Group through Bloomberg and Oxford Analytic to Stratfor. The cyber arena is a striking example of the change. In the traditional process, if a major hack occurred, it would fall to the Intelligence Community to attribute it to the perpetrator, then policy would decide on a response, name and shame, seek indictments or whatever. Now, however, that tidy process is disrupted, for while intelligence is doing attribution, so are a host of private companies. And they will not be shy about identifying the perpetrator, never mind what the government might prefer. In the short run, this seems competition; in the long I hope it will become creative collaboration.

- *Influence Operations:* One of my last duties as chair was overseeing the report to the president and president-elect on the Russian hack into the DNC emails. As the public version of that report portrays, it was pretty clear what Russia did. The attack had three elements: hacks into both parties but release only of material from the Democrats; an effort to invade infrastructure of elections; and traditional propaganda. In one sense, we had seen all this before. And, to be sure, the United States is no stranger to trying to influence elections or politics in other countries. But the new tools of the digital age make a difference, one of the themes of the conference.

- *Truth as Malleable.* So much for my list in normal times. It might be useful, even impressive, for my graduate students. Yet it seems overwhelmed now by the prospect that "truth" will be widely regarded as personal, or political or partisan. Mr. Trump's "false facts" are the poster-child, but the question is how deep and abiding this trend will be. Intelligence, still more than other endeavors, has always known how elusive the truth can be. And our language, like "true enough," is mirrored in the distinction between intelligence and law enforcement: true enough for policy is a looser standard than true enough for a court of law. (In passing, while I've come to admire the marble entrance to the CIA, I've always found the Biblical quotation from John odd and oddly placed there. In fact, and even in intent, intelligence's truth is more likely to constrain policy than to "set it free.") One of the great paradoxes of our times is that all the wonderful technology created to connect people has ended up segmenting them into "echo chambers" in which they hear only what they want and learn only what they already thought.

So far, I see no better response for intelligence than to double down on trying to distinguish what is likely true from what is not. False facts, in principle, make real ones more valuable, and their identification more pressing. The question is: will anyone listen? In the short run and for the Trump Administration, my guess is that the sheer complexity of the issues will turn it toward intelligence and toward a real interest in what is really happening. It is one thing to believe false facts about the turn-out at Inauguration but quite another to believe them while committing GIs to combat in Syria. Or at least I fervently hope so.

Discussion: The discussion picked up a number of issues. What is the role of the President's Daily Brief (PDB) – American intelligence's crown jewels – in the Trump administration. So far, the PDB is produced in two versions, one the traditional half dozen pages with about as many items; the other a one pager for the President. How American intelligence interprets information across cultures is an intriguing question, one worth more study. So, too, are the questions of how good more strategic assessments are, and how much used they are. On the former score, most academic studies of intelligence find it was pretty good in foreseeing the future. On the "how much used?" question, the 1991 U.S. National Intelligence Estimate on Yugoslavia is cautionary. It predicted Yugoslavia's violent future almost perfectly, yet had virtually no impact. It is a reminder that intelligence is, at best, only one of many inputs into policy; in the Yugoslav case it was overwhelmed by the mind-sets of U.S. officials (that Yugoslavia had fallen in importance with the end of the Cold War) and by the even more pressing need to tend to the disintegration of a much more important state – the Soviet Union.

Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case. This presentation laid out in careful detail the recent Russian record in influence operations. Those operations are relatively cheap, so they are a natural for a state that is, in many respects, a failing one.

- *Expanding in concentric circles.*[1] Surely, Russia is the poster-child for influence operations. It is hardly alone, though, in taking public diplomacy seriously. Since the inception of its English language TV network Russia Today in 2005 (now RT), the Russian government has broadened its operations to include Sputnik news websites in several languages and social media activities. These measures have been complemented with coordinated campaigns, using Western

1 For more detail, see Martin Kragh and Sebastian Åsberg (2017): Russia's strategy for influence through public diplomacy and active measures: the Swedish case, Journal of Strategic Studies,DOI: 10.1080/01402390.2016.1273830.

public relations firms, think-tanks and lobbyists to further Russian foreign policy goals. Moscow, however, has also been accused of engaging in covert influence activities – behavior historically referred to as "active measures" in the Soviet KGB lexicon on political warfare. Those have increased since Georgia and Ukraine. They have expanded in concentric circles – first against Russia itself and the domestic population. Indeed, one of the striking issues at the conference was whether Russian operations represented a resurgent Russia flexing its muscles or a weak one trying to bolster domestic support with nationalist action. The second circle is the post-Soviet space, the "near abroad," and the third, since 2014, is Europe and beyond.

- *Back to the Cold War.* Public diplomacy, like RT or Sputnik, is important but problematic. Like past Soviet propaganda, Russian public diplomacy today can also be wildly inconsistent. The West is portrayed as weak but at the same time as a near- existential threat to Russia. Europe is described as both xenophobic towards refugees, and foolish for allowing so many of them to seek asylum.i Russia's current approach seems back to the Cold War, with fronts, fake documents, and financing for sympathetic parties – all interconnected as "active measures."

- *Information warfare is part of national security.* Thus it is defensive, not offensive. Russia is under threat. It is meant to support Russia's interests, not necessarily Putin – to get sanctions removed or support Russia's annexation of Crimea. This lineage runs far back, to the Protocols of the Elders of Zion in Czarist times before World War I. And Russia efforts can draw on sources closer to home: Russia alleges that the CIA killed JFK, but Oliver Stone's movies come close to making the same point. Trying to plant stories in legitimate media was not easy. Social media makes it much easier. Still, Russia has planted a number of forged documents, ranging from Sweden appropriating fertile soil from Ukrainian farmers, to Poland lambasting the Swedish government for the country's neutral position during World War II to the civilian nuclear energy company Westinghouse fomenting nuclear accidents in Ukraine with its sub-quality fuel produced in Sweden. Carl Bildt, the former foreign minister and critic of Russia, is the most frequent target of Soviet measures. That said, there is no evidence of that Russia's measures have had an effect on strategic decisionmaking in

Sweden. That is a contrast to other countries, where some parties actively support the Kremlin.

- *Convergence of right and left.* Russia is active with groups on both the right and the left, and the two often work together. For instance, as elsewhere in Europe, RT and Sputnik in Sweden have attracted readers and contributors from the far right, the far left, populists, libertarians, conspiracy theorists, Wikileaks supporters, peace organizations and environmentalists. And the Russians play hardball, as the presenter could attest, seeking to discredit those who uncover Russian influence operations. A Finnish colleague, Jessikka Aro, was slandered from both the right and the left. What happened to the presenter was perhaps less, but still ranged to death threats. He was reported to his university, Uppsala, for academic misconduct, with the allegations coming from both sides. There was really nothing specific, and nothing really related to scientific misconduct. Still an investigation ensued, and it was reported by the quality media.

Discussion: Why was there an investigation at Uppsala? Why did the university fall into the trap? The answer turns on institutions and procedures created in different times for different circumstances; in the same way, a major freedom of information request could virtually shut down the ministry of foreign affairs. In contrast, when Russia tried its allegations of rapes in the Baltic by NATO soldiers, Lithuania was ready. Its parliament immediately dismissed the story as spurious. In that sense, the Baltics can provide some lessons, given their long experience with the Russians. Still, open societies are inherently vulnerable. Is it important to attribute attempted disinformation to Russia? Disinformation probably should be treated the same way no matter what its origin, for Russia and others can always outsource, paying a Macedonian company in bitcoin for false stories.

During the Cold War, the Russian SVR had an office of influence ops. Now there are new tools, like social media and cyber, and it is easier to move money. But there is also enough continuity so that attribution to Russia is possible. How can we distinguish directed from like-minded but independent journalism? It is indeed hard to distinguish clueless journalists from those who are paid or are ideologues. It is important to look at the combination of military or physical and information realms. For instance, Russian propaganda started in 2013 and could have alerted to us to the military threat to Ukraine. Russian doctrine makes no distinction between military and information. Are we losing the information war? Let us hope not. In any case, "balanced journal-

ism" can mean giving equal credence to a lie – such as the BBC giving almost as much coverage to Syrian denials that it was responsible for the chemical attack as to the attack itself.

Influence Operations from a Scandinavian Perspective. The Russians are good at targeting their influence operations, for the target is not really "northern Europe" but rather the Baltics in particular, given their history and populations. Again, it is difficult to separate Russian proxies from sympathizers.

- *Differences across northern Europe.* As figure 1 suggests, there are considerable differences across northern Europe in the extent of Russian interest and thus targeting of influence operations. There is less covert influence in Denmark and Norway, but slightly more in Finland and Sweden, though the two latter differ as well. Sweden has an open debate climate, one that is used to things being brought up. However, its equality is probably a negative from the Russian point of view. By intent and design, Russian actions seek to influence both Swedish views of Russia and Russian view of Sweden. Those actions play on polarization to diminish the credibility of Swedish and European institutions. They try to mobilize those who already harbor a negative view of, say, NATO.

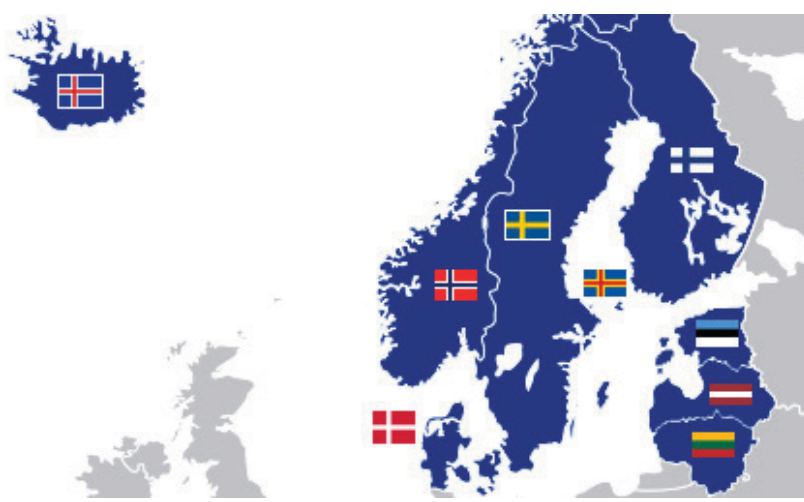

Figure 1: Northern Europe as a Target for Influence Operations

- *Swedish vulnerabilities.* These include lack of awareness and understanding of what Russia is up to. That is getting better but slowly. Social trust among Swedes is high, though that is less the case for the young. The practices of journalism make it hard for journalists

to do criticism of sources. That is all the more so when information operations play on pre-existing social stressors and play off the new information structures: notice that the flash stock market crisis was set off by two sentences on a web site.

- *Response versus resilience.* In the short run, responding means using existing legislation to develop strong links between government and society institutions. It calls for clear communication, and efforts to enable media to be better at delivering context. It is important to analyze new media platforms before using them, but also to act quickly in new media, exposing methods and links. That said, long-term resilience-building should be the priority. That, in turn, requires demanding action from social media and search engines to better police their content; seriously conveying the story about Sweden; and strengthening both government and civil society institutions for countering influence operations.

As others mentioned, whether and when to respond is a critical issue. It is always tempting to respond – a kinetic example was IEDs in Afghanistan. But if opponents can saturate the information environment, we could spend all our time chasing balls. We should look at what we can do, not what we can't. Should we call the combat of influence operations "war"? The question is complicated. For Ukraine, a "yes" answer seems correct, but that can play into opponents' hands. A cautionary example is perhaps the Swedish military, which is not so esteemed as in Britain; it not clear why it is in Afghanistan. So identifying information operations as war may overemphasize the role of the military. The police are critical too. What is needed is a broad effort, by government and society, not a narrow departmental one.

Discussion: Liberal democracy is under challenge in many places; polls show, for instance, that young Americans are less attached to democratic values than their elders. That challenge is played on by the Russians and others. Should talk up our narrative, but how? What is line for accepting versus combating influence operations? We are taking it on the chin, but will be only underscore the effect by combating? In any case, we need to know the target audiences. Who is disenfranchised? Russia has been active since 2014, so there is no element of surprise. Yet so, too, is there no quick fix. It is a worry that Russia has a more strategic approach. An example is migrants across Russia's border with Finland – Russia drove home the lesson that they could turn the flow off and on. In Sweden, people are trying to rescue symbols, like the flag, from the ultraright. One issue for governments is how to go public, and how much to share across agencies, without risking sources.

Commentary and discussion. The commenter generally agreed with the presentation, and so turned to devil's advocacy. First, how to frame the issue or narrative? Is what we see the result of an aggressive Russia or a weakened and defensive one? He thought the latter. Russia is not a failed state, but it is close, and we should avoid playing into the strong, aggressive narrative. Second, how much are the operations directed at the Russian population and how much at us. Putin casts himself as the defender of Christianity, gets support, and so is much of what we see designed to bolster him internally despite catastrophic policy? Third, there are the plain idiots, like the American who came to Washington with a rifle to liberate children who he had seen on the web were being victimized by a ring led by Hillary Clinton and run out of a pizza parlor. It is simply too tempting to try to exploit our vulnerabilities.

Fourth, some historical perspective is apt. At one point, Britain was very good at covert influence operations. Then, though, the military turned toward the revolution in military affairs and technology. But, as the presenter argued, this is not just a military issue, an extension of psyops. It requires a whole of government approach. Working from a military base got John Poindexter in trouble in the United States a generation ago. His Total (later "Terrorist") Information Awareness program was an idea ahead of its time. Fifth, we have advantages because we understand digital tools better than our adversaries if we choose to use them. So far, we have not really chosen to do so, and the counter argument would be this is dangerous, trying to influence our own people. Another of our advantages is a free press. Wikitruth is a nice example. Finally Russia does create noise in addition to deception. Much as magicians divert to deceive, how much of Russian noise is intended to distract and why, say, to distract from its calls for weapons free zone in Baltic?

What do we have on the shelf? There was a rebuttal unit in NATO re Kosovo that sought to counter the Serbian narrative that a hospital was bombed on purpose. But what response to what? It is useful to distinguish government and state media responses from clandestine or other unattributed responses. The former can be done without panic. That latter does run the risk of encouraging those who are crackpots, not just gullible. It is important not to see a master plan behind the crackpots. Again, Russia's activities are both foreign *and* domestic policy; the key is keeping Russian society in a bunker mentality. In summing up, the discussion raised four issues: how easy or difficult is attribution? What is the target, us or Russian society? How effective are the operations? It is easy to overstate their impact; so far they have influenced mostly the already converted or sympathetic. How do we assure that we don't

damage our democracies in the effort to protect them? That is a special issue as we deal with the "idiots."

Session 2: Who Needs What to Counter Unfriendly Influence Operations

Securing the State from Offensive Cyber Influence Operations. A generation ago, the focus turn to the jihadis, and secret intelligence was key. Now cyber is very much on the radar, including in the realm of offensive influence ops. And intelligence is still central.

- *Weaponizing information.* For instance, Snowden was a weaponised whistleblower, not a Russian plant but a man groomed by hostile media then adopted by Assange to become an unconscious agent of influence for the Russians. He was an atypical leaker: a right wing "patriot," what originally upset him was the government, through NSA, spying on American citizens in a way that he believed was unconstitutional. A number of factors contributed to this damaging episode: post 9/11 criticism of "Need to Know" and the move to "Dare to Share"; contracting out of a highly sensitive intelligence task; weak security procedures in both NSA and the private sector; and too much secrecy over the existence of domestic surveillance

The Snowden leaks have damaged vital intelligence collection including in support to military operations. Moreover, much of the material is hard for journalists to interpret, making it all too easy for media and civil liberties groups to exaggerate, leading to charges of widespread illegality by agencies – shown by courts to be false but widely believed. Britain, at least, has legislated to increase the transparency required for the modern rule of law, but the ECHR and European Court cases continue. And the Russians are exploiting the embarrassment. One group, calling itself the Shadow Brokers, hacked an advanced cyberespionage actor, the Equation Group, believed to a cover for NSA Tailored Access Operations. The Vault 7 leak exposed CIA tools. The leaks have caused both operational and diplomatic damage. Internet companies are playing hard to get. To boot, the exposures have made clear how far some nations were behind the United States and the Five-Eyes, encouraging them to develop their own capabilities or to buy in capability, for example in social media and mobile phone monitoring. Several European nations are considering whether their legal frameworks need to be updated especially for bulk access; but some seek to inhibit digital intelligence. After going through several phases, Britain

accepted in 2017 that it had to find an intelligence model that commanded public support.

- *Info Ops and 'Agit-Prop.'* These operations have a long history, one running, in Britain, back to the 1924 Zinoviev forgery, to discredit the Labour Party. The 2016 American elections were, however, a modern turning point. The United States judged the operations to be the responsibility of the Russian state. As earlier discussion indicated, the Russian audience is domestic as well as foreign, and the activities cover a wide range, in addition to the hacks as an example of weaponizing information:
    - Military operations such a intrusions into airspace and overflying exercises for signaling resolve;
    - Expansion of conventional digital media operations (RT, Sputnik);
    - Subversion via social media blogs, websites;
    - Covert actions to discredit/kill opponents;
    - Offensive cyber operations

The Russian attack on Paris TV5 raised questions why and how competent? If the effort was to indirectly influence policy by discrediting Hollande, *Paris Match* did better!

- *Russia is hardly alone.* China's PLA Unit 61398 – '"Comment Crew" – is the 2nd Bureau of the Chinese People's Liberation Army's General Staff Department's 3rd Department. Its main location is known. The most troubling attack to date by Comment Crew was a successful invasion of the Canadian arm of Telvent. The company designs software that gives oil and gas pipeline companies and power grid operators remote access to valves, switches and security systems. Telvent keeps detailed blueprints on more than half of all the oil and gas pipelines in North and South America, and has access to their systems.

For China, the aims are to distract from, say, its actions in the South China Sea or to add cyber friction in the event of conflict. North Korea attacks banks for the "Willie Sutton" reason – the money is there and the hacks have produced big money for North Korea. As President Obama put it: *"Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems."*

- *Fake News Is also a Domestic Issue.* Witness the memes attributed to President Trump. In effect, real news media are surrounded by the fake news ecosystem, which is a micro-propaganda machine, rife with conspiracy theories and paranoia. See figure 2:

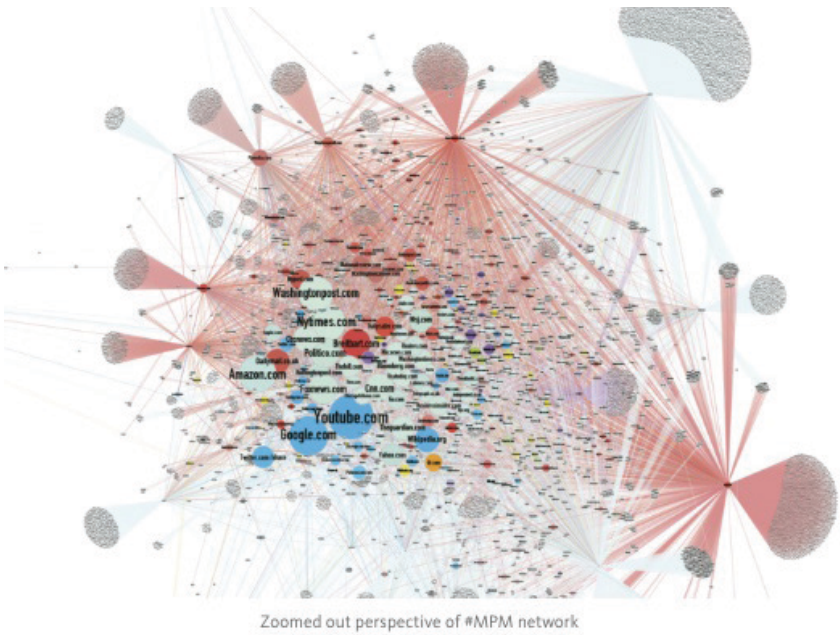

Figure 2: Real News Media Surrounded by Fake News

- *What to Do?* A number of themes recurred, though with a sharp cyber emphasis. Strengthen national cyber defenses overall including active defenses; more emphasis on personnel security and care over contracting-out; seeking to identify hostile information operations must be an intelligence priority; analysts must be trained to expect deception and stick to intelligence principles in assessment; use intelligence assets to be ready to advise on attribution and identify and name key actors/groups; build offensive cyber capabilities to provide policy options and plan for other responses; improve critical infrastructure and cyber protection; organize at NATO and government level to rebut propaganda and fake news fast; work with Internet companies to have illegal material taken down faster; improve our own public narratives and win the key arguments with our publics; encourage good journalists to investigate and expose what is going on, and not to be artificially even-handed; support

overseas broadcasting to Russia; develop public education on the risks of the digital world, starting in schools, including spotting "alternative facts."

Discussion: Offensive cyber does have some deterrent effect, though not in the same way or extent as nuclear weapons. In designing cyber responses, legal issues would be case by case, if, for instance, the responder wanted a front company at home or in an ally. One tack is to Infect so attacks are easy to attribute. What about our disinformation? Now, there no space for covert operations, though there was in pre-digital era. We can't risk the loss of confidence in journalism, for the free press is critical for us. As another cautionary example, black ops were tried in Northern Ireland, but the Army realized it was a mistake, because they had lost journalists' confidence. Nor should governments use third parties. The Stansfield Turner standard is the one to apply: don't do if you're not prepared to see it on the front page of the *Washington Post.* Operators have redefined secrecy and now admit to hacking etc.; they wouldn't have before. Attribution incorporates two parts – the intelligence assessment, where there is always some uncertainty – then the political decision to go public. Attribution is best if its finds stuff that has been hacked. Attribution through code harder but doable; the Cyber Caliphate is an example.

Dissemination to whom and how to counter influence operations. This presentation underscored some of the themes that had run through the conversation. Some of the challenges include having to deal with "alternative facts" and "fake news," along with explosive growth in forms and numbers of social media. Notice Stalin's refusal to believe all the evidence that Hitler was about to attack: fake news can mean it's true but don't care. That then plays on the increasing public alienation from established media. In the last election, most young Britons got their information entirely from Facebook.

The "Kardashian culture" is fertile ground for our opponents. For young people, the Cold War is ancient history, and so they are The younger generation is unaware of threats from past protagonists, and so lacks firm reference points. They are tempted to believe the person making the most extreme point, a temptation that can be exploited ruthlessly by opponents, which then leads to instant world-wide coverage. And it gets worse. Our opponents no longer play by the rules. We know who some of them are, but not all of them. They can get there before we can, and they are everywhere and we are not (yet). "A lie is half-way round the world before truth has its boots on…" – a quote variously attributed to Thomas Jefferson, Mark Twain, and Winston Churchill. Our opponents have immense credibility and any response we make will be

discredited. Moreover, no one feels the pain of the attacks until they do. So what can we do to turn the tide? Where to start?

- *Nine points to begin*

  1. Existing crisis management operational structures: Are they adequately configured? Can they deal with war, terrorism, catastrophic civil events? Can they be adapted for new threats of influence operations?

  2. Assessment and calibration of threat: State and/or non-state actors? Targets – military, civil, private sector assets, civil society and individuals? Frequency and length of attacks? Political and election campaigns? Subversion + deflection? Sabotage + active disruption? Denial of service? Kompromat and intrusion?

  3. Our capabilities: Military or civilian assets? Intelligence services? Open rebuttal/denial? Who makes the judgments?

  4. Identifying response options: Evaluation of % chance of success? Risk analysis? Probabilities of retaliation? "Profit and loss"?

  5. Legal authority: Depends on nature of threat? "Undeclared warfare"? Rules of engagement? Who decides legal basis? Existing political + decision making structures adequate? Existing mandates/new authority? Legislative and policy directives? Have you codified all this?

  6. Political/public understanding: Ministers and politicians General public and individuals Alertness and awareness of risk Unfamiliar and scary stuff...Dense technical issues…

  7. Political decision taking: Existing structures? Speed and depth of response? Judgments on risk and capability?

  8. ISPs and private sector interests: Likely to affect their interests and operations? Financial implications if systems taken out? Should they be involved and if so how?

  "We cannot become arbiters of truth ourselves. It's not feasible given the scale and it's not our role" *Adam Mosseri, Vice-president of news feed, Facebook*

"If they really want to tackle fake news, they could get their teams and algorithms to identify and blacklist the people who put out these stories" *Zoe Cairns, social media expert*

Consent or legal enforcement? Financial penalties for non-compliance? Worst-case scenarios – ISPs complicit? If they are unwilling to engage…?

9. Media lines and declarations of activity: Activity totally covert like all intelligence operations? Any value in declarations of activity? Silent and reactive or proactive? National Security Strategy National Risk Register How to present this publicly? How to finance it against many other resource demands?

- *Britain's response*: "We have launched the new National Cyber Security Centre to lead our response to the increasing threat from cyberspace" – UK National Cyber Security Strategy 2016. The strategy is comprised of three basic elements: Defend; Deter; and Develop (increasing resilience). The program is driven by twelve basic questions:

  - Analysis and understanding of targets?
  - Response capabilities?
  - Are cyber strategies sufficient to counter influence operations?
  - Active countering?
  - Aggressive or subtle?
  - Response times?
  - Confront and deny?

  - Extent of awareness?
  - Public confidence in our response?
  - Target hardening and asset protection?
  - Costs – who pays?

  - Job for politicians or for intelligence experts?
  - Location of your response options?
  - Plans and exercises?
  - Worst case scenarios?
  - National perspective on resilience ?

- *Can this work…?* The challenges are the ones that recurrent throughout the conference. Open societies are inherently vulnerable, yet it is imperative that they stay open. So, too, parliamen-

tary democracies can be slow and cumbersome, but they too are imperative. It is also imperative to protect free speech, and to remember that it is not the state we are trying to protect, but rather its citizens. The British approach is a whole of government on. Its core is COBRA, the cabinet office briefing room, a crisis center. The very name COBRA encourages attention, and so whether or not it's up and running, and which officials are attending: these are themselves newsworthy. It starts with the intelligence assessment. The process is trial and error. For instance, it was first applies to the 2008 financial crisis, but didn't really work – the crisis was longer, plus it was necessary to engage industry leaders, for whom the setting was uncomfortable.

Discussion: Nothing much is very secret about Russian influence operations. German Chancellor Merkel is said to have told Putin directly not to interfere in German elections. So too the 2015 attacks on the Ukraine power grid was pretty much in plain sight. We ought to be creative in thinking about response options. What about billion dollar bond for ISPs? They would get it back if they were judged good at policing their content. It's outrageous in current circumstances but worth thinking about. Or in the past governments have prearranged panels of scientists to be consulted if need be. What about an advertising executive panel to assess messages? Do we abandon truth? It sometimes feels that way. We grew up with responsible media, so have to come at it afresh. Especially, we can't surrender our strengths.

Concluding themes.

- *Public-private.* Not surprisingly, much of the conversation was about how to work across the public-private divide. The Cold War, especially its nuclear component, was a government monopoly. Not so now, when not only are national infrastructures in private hands, but the information was is explicitly fought over the minds of the people.

- *Convergence of cyber security and influence operations.* We started with the latter and ended up concentrating on the former. That, too, is perhaps not surprising, for not only is the cyber domain critical, but much of what's new in influence operations is digital: witness the ease of putting things on the web by comparison to the difficulty of planting stories in newspapers.

- *What next?* This convergence raises the question: what is the next big thing? Governments and their legislatures should be in front. For example, what about Artificial Intelligence (AI) in the cloud able to identify people with a fleeting glance. Swarms of drones could be looking for criminals and terrorists, while China was looking for dissidents in Hong Kong.

- *Keeping the web whole.* Russia and China want their own internet, but our long-term interest argues for an open internet. This is an enormous issue, one that hearkens back to the work of the Bildt reports some years ago. We can't keep out bad guys, so the issues becomes what they find when they get there.

- *Impact of influence operations.* For millenials, the impact of influence campaigns is hard to calibrate. That issue recurred; it raises the question of how much intelligence services should reorient themselves to deal with it. Is problem worst now, will it get better as people get used to Russian interference, and recognize it? Will it become self-inoculate?

- *How to respond?* This came up again and again. There will be cyber attacks, so we have to calibrate what's important and what is less so, when to talk openly and when not. How to increase the cost to Russia? We can do better at defense but need to to increase cost. The recent U.S. agreement with China not to do cyber espionage for commercial purposes, is a start; Britain and Australia also came to similar agreements with China. Still, can the cost to Russia be raised high enough? A clear red line would be interfering in elections. In the Cold War, Britain once expelled 100 Soviet agents at one time. What about the money trail? Where is Putin's? In the end, we want to get rid of real but offensive and criminal facts, like beheading, so this is not just about false facts.

- *Cooperation and whole of government.* Russian influence operations require trans-Atlantic coop, which Putin tries to break. Internally, Sweden and Britain are perhaps more alike than it seems. Sweden had the concept of ad Total Defense, but drew it down; it had a civil agency thinking full-time about influence, but it only had a mandate in wartime. Russia will continue to look for seams in legal systems: the Georgia issue in 2008 came back to U.S., servers in Austin. In the end, the role of intelligence in influence ops is still an open question.

Influence Operations and the Intelligence/Policy Challenges

This conference report aim to assess influence operations, especially those conducted by Russia, in the context of changing relations between intelligence and policy and the emerging challenges for intelligence. Three key challenges were discussed in regard to influence operations. First, *Identify* – how to separate state sponsored disinformation from individual rumor mills. Second, *Understand* – how to understand influence operations, put it into a context for policy makers, and learn to understand the underlying factors and why it happens. Third, *Counter* – how to vaccinate civil servants and enhance the critical approach within media to create resilience against influence operations.

The first part of this conference report lays out on how to identify and understand influence operations in the context of policy. The second part focus on who needs what to counter influence operations. The last part contains concluding themes.

Dr. Gregory Treverton is the former chairman of the U.S. National Intelligence Council, as well as former Director of the RAND Corporation's Center for Global Risk and Security. Dr. Treverton is also a Senior Fellow at the Center for Asymmetric Threat Studies (CATS) at the Swedish Defence University.

ISBN: 978-91-86137-66-3

Swedish Defence University
Box 278 05
SE-115 93 Stockholm