Intel-for-Hire Undermines U.S. Intelligence (Part 2)

Intel-for-Hire is a multilayered phenomenon that's undermining the integrity of U.S. intelligence, argues George Eliason. In this installment, he looks at the second tier of this system. (Click here for part one. Part three is here.)

By George Eliason

In part one of this series, we looked at the top level of the privatized intelligence community showing that large for-profit companies and individual actors have other interests in mind than the public good. Work that was previously considered inherently governmental is routinely contracted out to people who only serve their own self-interest, which may be at odds with what most people might expect from intelligence – for example, unbiased information to guide sensible policy-making decisions.

Now we'll look at the next level down – the smaller companies, specialty companies, and practitioners that service the top level. We'll see how they fit in the picture and work in real life.

In 2016, Tim Shorrock wrote an article describing the five intelligence giants that control domestic policy, foreign policy, military, and civilian leaders with the products they sell. They create the information, analyze the information, and decide who the President of the United States will see as an enemy and who as a friend.

The smaller companies provide the resources for them to work with and base their reports on. In the digital age intelligence has become a buyer's market. If the larger company profits more by finding Russian influence at work at a grammar school Christmas play, then that's the conclusion that will be drawn. If you aren't up to the task, someone else will provide the "proof." After all, that's where the money is.

One of the main players in this process is the Chertoff Group, founded by former Secretary of Homeland Security Michael Chertoff. From the Chertoff Group,

through the Alliance for Securing Democracy, through the German Marshall Fund of the United States, and through the Hamilton 68 Dashboard – which purports to track "Russian influence operations on Twitter" – the information is distilled and passed down to the mid-level players.

Michael Chertoff from 2005-2009 ran the massive Department of Homeland Security, where he was criticized for exempting the DHS from following laws on everything from the environment to religious freedom. A report issued by the Congressional Research Service said at the time that the delegation of unchecked powers to Chertoff was unprecedented. He was also known for railing against international law, warning that treaties such as the Geneva Conventions were placing undue constraints on U.S. actions abroad.

As a long-time insider – in both the public and private sector – he is one of the top figures in the U.S. intelligence-security complex.

U.S. (and Foreign) Government Contractors

Private sector services mirror what they do for government including Intel-for-Hire, espionage, information operations, direct action, and state-sized propaganda operations. This is work that the government has stated on many occasions needs to remain with the agencies that can be held responsible to the public – and not to private companies that aren't.

The contractors and companies work both inside and outside U.S. government circles. They sometimes work for foreign governments. When they are in the private sector, they have no problem attacking and harassing U.S. citizens as well as the rest of the global community. Wherever their clients point, they fire.

This is the part some of the worst offenders take very seriously. In their world, they are James Bond and destroying the reputations of innocent people is a service to their country, and keeps their bank accounts flush with money. In their minds, they are this generation's super-patriots, when in fact, as soon as what they do is opened to inspection, they are common criminals.

People with no security clearances and radical political agendas have state-sized cyber tools at their disposal and can use them for their own political agendas, private business, and personal vendettas the same way they use CIA's Vault 7 hacking tools for state projects. And this has been going on for years.

In a Sept. 2013 Reuters article, Jameel Jaffer, deputy legal director at the American Civil Liberties Union, said the reported incidents of NSA employees' violations of the law are likely "the tip of the iceberg" of lax data safeguards. The laws guiding the NSA's spying authority in the first place are a

bigger issue, he said. “If you only focus on instances in which the NSA violated those laws, you’re missing the forest for the trees,” Jaffer said. “The bigger concern is not with willful violations of the law but rather with what the law itself allows.”

The companies and individual actors sell information. For some, this is the basis of how they market their services. They spy on other companies – on regular people – commit espionage and run legally dubious information operations against civilians.

But because of the work they do for both the U.S. government and private corporations, few restrictions are placed on them. Where they are supposed to be supervised by the Director of National Intelligence (DNI), in some cases they are supervising themselves and other companies and training DNI agencies to act like them.

Anything marked as “intelligence” is also designated top secret by the all of the DNI agencies, so even something that is originally open-source information becomes “top secret” once it is earmarked for an agency. This is being done on a regular basis at different levels.

Legal Gray Zones

Although some laws are in place restricting these activities, there are legal gray zones that these intelligence players skirt around and operate in when committing acts against the American people. They have identified the key areas of the law and made sure there are built-in loopholes, which Congress keeps in place following hearings at which these people often testify as expert witnesses.

In some cases, they wear their chutzpah on their sleaves.

On September 21, 2015, Joel Harding, who describes himself as an “Information Warfare and IO expert, Strategic Communications, Cyberwar, Ex-Special Forces,” posted an advertisement making clear the brazenness with which these privatized spooks operate.

“Ladies, Gentlemen, and everyone in between,” he wrote. “I am building a database of planners, operators, logisticians, hackers, and anyone wanting to be involved with special activities I will call ‘inform and influence activities’.”

He noted that he had received various suggestions to help organize operations against “anti-Western elements.”

“No government approval, assistance or funding,” he claimed. “This skirts

legalities. This is not explicitly illegal and it may not even be legal, at this point. That grey area extends a long way." In soliciting resumes, he told prospective partners that if they "have hands on experience of a less than legal nature, you might not want to admit illegal work."

The first industry hotshot to jump up to help was Andrew Weisburd.

Together with Clint Watts and J.M. Berger, Weisburd has testified to Congress as an expert from the intelligence and security industry. To advance their industry's profitability, they work with friendly lawmakers to widen those legal gray areas.

Lawmakers, in turn, collect hefty campaign contributions from the industry. In addition, they sometimes get to hear and see intelligence that they may not be authorized to hear and see. Since senators and congressmen are not permitted to look at classified intelligence outside of their mandates on particular intelligence committees, the system of Intel-for-Hire enables privately gathered intelligence to make it to congressional eyes before it is classified.

Outsourcing Intelligence

Despite lacking professional credentials, a commitment to public service, or the minimum amount of vetting that would go into a security clearance background check, these private-sector spies collect intelligence that is passed along and ultimately may be included in the President's Daily Briefing.

In other words, consultants and "public affairs professionals" with little actual experience in the professional intelligence community – some of whom may have an axe to grind or are just trying to make a buck – can help decide who is an enemy of the state. That's the reality we are left with even though it sounds like a surreal B-grade movie.

If Weisburd or his partner Clint Watts sound familiar it's because it is their work testifying in front of Congress in the spring of 2017 on Russian influence on the 2016 election and in social media that is pushing policy and leading us into a new Cold War.

Weisburd and Watts have also established much of the groundwork on which every other Russian menace story – attacking Ukraine, hacking elections, etc. – is based on. Their idea of countering Russian influence has been to take out American, Canadian, and European English language websites owned by citizens of those countries. As Joel Harding's slogan makes clear, it is a strategy based on information warfare: "To Inform is to Influence."

Here's how the parts tie together.

These experts are the “small players” that developed the Hamilton 68 Dashboard for the German Marshall Fund, which is part of the Alliance for Securing Democracy that Michael Chertoff advises.

The dashboard is “an interactive dashboard displaying the near-real-time output of Russian Influence Operations on Twitter—or RIOT, if you’re a fan of on-the-nose acronyms,” according to J.M. Berger. He says that it’s the product of a research collaboration that includes himself, Clint Watts, Andrew Weisburd, Jonathon Morgan and the German Marshall Fund.

So now we have Michael Chertoff advising and supporting the work of Weisburd, Watts, Berger, and possibly Weisburd partner Joel Harding.

It’s just a fact of life at some point, somehow, somewhere, someone is going to take a look at the quality of the work you do and decide if it was worth hiring you or if you are just another scam story trying to stay on the federal dole.

This is that day for the Hamilton 68 Dashboard crew.

Upon closer inspection, it’s a safe bet that many of the people called “Russian trolls” that are allegedly destroying American democracy aren’t Russian or on Russian payrolls at all. They are Americans expressing political views and sharing articles.

The sampling that Clint Watt’s and Andrew Weisburd’s failed Hamilton 68 Dashboard uses is tiny and easily skewed. If a handful of people can generate the second highest hash tag position, the “real time” tracking of Russian propaganda is totally undermined.

More troubling, in recent years more of these Intel-for-Hire contractors have gone offline working with direct action units in other countries that are committing murder. More on this in a later installment.

George Eliason is an American journalist who lives and works in the Donbass region of Ukraine. For part three of this series, please click here.