West makes concerted counter-strike in wake of Russian spy poisoning

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

The Russian nerve agent attack on Sergei Skripal and his daughter has fundamentally altered the West's approach to dealing with Russian provocations. *James Bingham* analyses the forms that the counter-strike is taking

Key Points
- A concerted US- and UK-led pushback by Western states has begun against provocative Russian intelligence and disinformation activity, apparently concentrating on exposing the shortcomings of the GRU.
- Future Western responses are almost certain to involve diplomatic, economic, and communications strategies; offensive cyber operations against Russia are highly unlikely in the short-to-medium-term outlook.
- An enduring operation by Western states to collect further intelligence on Russian intelligence activities and to selectively release compromising details that previously would have remained classified is likely.

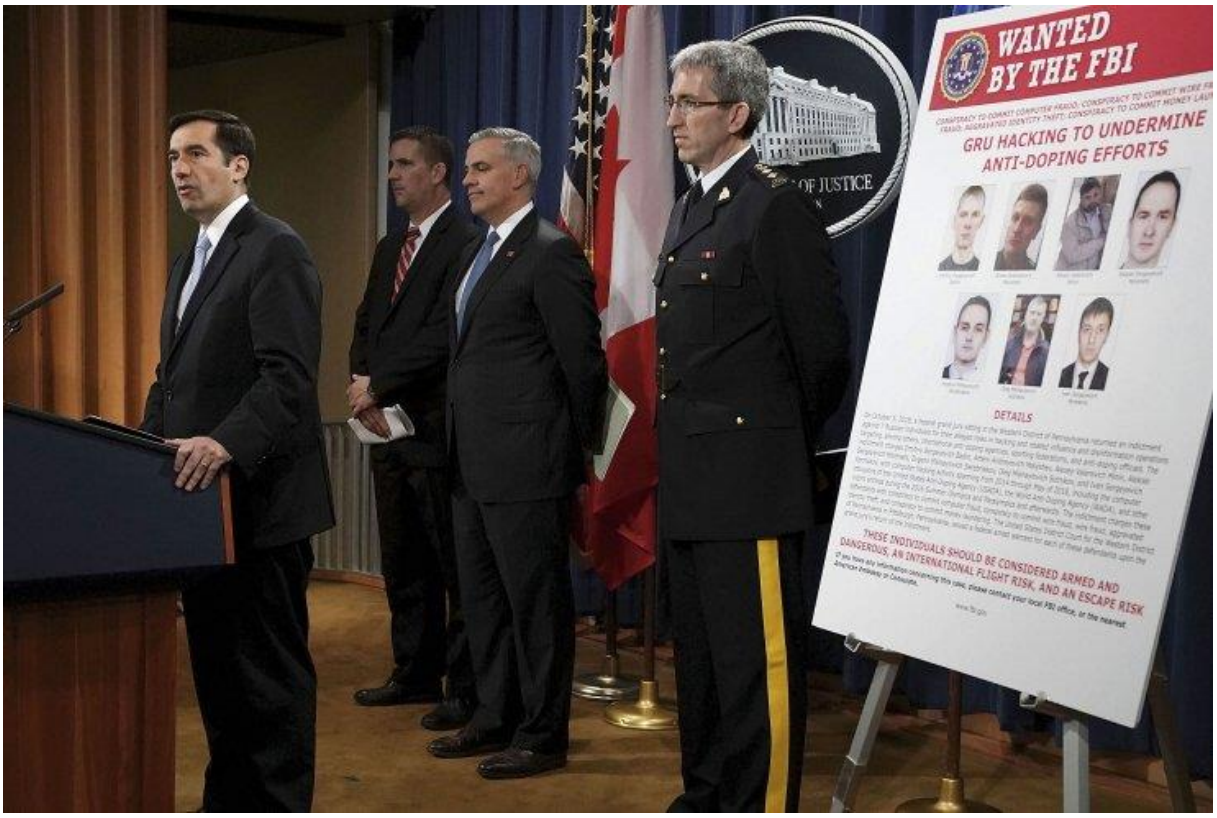
The attempted Novichok nerve agent assassination of former Russian spy Sergei Skripal and his daughter Yulia in Salisbury in March 2018, and the subsequent death of UK citizen Dawn Sturgess, marked a turning point for the West and its relations with Russia.

Jane's understands from sources close to a Western intelligence organisation that the episode was viewed as a provocation too far, prompting a multinational determination to respond to Russian intelligence activity, with a focus on increased inter-agency co-ordination. Confirming this new approach, but commenting on a separate intelligence case involving Greece, FYR Macedonia, and Russia, *The New York Times* on 9 October reported former US ambassador to Macedonia, Christopher R Hill, as saying, "We're pushing back and showing that we can play hardball too… We can tattletale, we can do things that maybe in the past we did not do."

In the Skripal case, the first visible countermeasure was the closely co-ordinated mass expulsion of 155 Russian officials by 29 countries and NATO in late March – the largest in history. After Russian counter-expulsions took place, a period of relative diplomatic calm ensued, during which *Jane's* judges it highly likely that preparations were co-ordinated by the UK and US – involving numerous Western states – to begin implementing a 'counter-strike' involving diplomatic, economic, intelligence, and cyber options.

The dispute reignited on 5 September, when UK Prime Minister Theresa May named Ruslan Boshirov and Alexander Petrov as the Russian military Main Intelligence Directorate (Glavnoye Razvedyvatelnoye Upravleniye: GRU) operatives responsible for the failed operation, an identification also publicly confirmed by the head of the UK Security Service (MI5), Andrew Parker. On 6 September, confirming the West's resolve to respond, UK Minister of State for Security Ben Wallace declared in a radio interview, "We choose to challenge the Russians in both the overt and the covert space, within the rule of law and in a sophisticated way."

Subsequently, on 26 September, the online investigative sites Bellingcat and The Insider revealed that they had "established conclusively" the identity of Boshirov as Colonel Anatoliy Chepiga, "a highly decorated GRU officer". UK government security sources did not dispute that identification. Bellingcat on 9 October then identified Petrov as GRU military doctor Alexander Mishkin. Nevertheless, Russia has consistently denied responsibility for the poisoning, and the two men claimed on Russian television that they were simply tourists.



Assistant US Attorney General for National Security John C Demers (left) announces criminal charges on 4 October 2018 in Washington, DC, against seven Russian GRU intelligence officers for their alleged roles in hacking and related influence and disinformation operations targeting international anti-doping agencies, sporting federations, and anti-doping officials. Underlining the international nature of the response to Russian provocations, Director General Mark Flynn of the Royal Canadian Mounted Police (right) also attended the conference. (Alex Wong/Getty Images)

1726444

On 4 October – in the clearest indication to date of a tightly co-ordinated multinational response – three near-simultaneous revelations again placed the GRU in an uncomfortable spotlight: the UK accused the agency of numerous cyber attacks; the Netherlands revealed the detention in The Hague of four GRU officers accused of attempting to hack into the Organisation for the Prohibition of Chemical Weapons (OPCW); and the US Department of Justice indicted seven Russians for cyber plots against various targets.

Significantly, the revelations drew attention to numerous and easily avoidable failings in GRU operational security (see box), with a level of detail usually not cleared for public release. From the events to date, *Jane's* assesses that further public releases to embarrass the GRU are highly likely, and that the focus will remain on the GRU rather than other Russian agencies in an attempt to sow discord within the competitive Russian intelligence community.

Implausible deniability

Keir Giles, a senior consulting fellow of the Russia and Eurasia Programme at Chatham House, London, told *Jane's* on 11 October, "The unprecedented transparency shown by the Netherlands intelligence services in exposing Russian GRU officers confirms the new trend in the handling of offensive activity by Russian intelligence… [US and UK initiatives] have set precedents for revealing information that previously would have been confidential."

Furthermore, Emily Ferris, a research fellow in international security studies at RUSI, London, told *Jane's* on 15 October, "It is highly likely the GRU will continue this level of activity, mainly to probe other countries' defences … some of the mistakes made by the GRU are not reflective of the agency's broader capabilities to conduct operations abroad, which are very good."

Russia has operated 'deniable' operations within the borders of Western states on numerous occasions, including the poisoning of Alexander Litvinenko in November 2006 with the radioactive substance polonium-210. However, the use of the military-grade chemical weapon Novichok on British soil has been framed in public discourse as a turning point for Western responses to Russian foreign operations.

A joint statement by the US Department for Homeland Security (DHS) and Federal Bureau of Investigation (FBI), along with the UK's National Cyber Security Centre (NCSC) in April 2018 identified how Russian government operatives had targeted "government and private-sector organisations, critical infrastructure providers and the internet service providers [ISPs] supporting these sectors" with "malicious cyber activity". The indictment of 12 Russian individuals by US Special Counsel Robert Mueller in July, following the 2016 hack of the Democratic National Congress (DNC), as well as the public exposure of a complex counterintelligence operation leading to their identification, also identified the GRU as the principal body responsible.

The US Office of the Director of National Intelligence (ODNI) also concluded in January 2017 that the Russian government had used covert intelligence and overt disinformation campaigns to assist the presidential campaign of Donald Trump. Furthermore, the ODNI assessed that "Moscow will apply lessons from its Putin-ordered campaign aimed at the US Presidential Election to future influence efforts worldwide".

The context is the ongoing and multifaceted components of Russia's cyber and disinformation campaign preceding the 2016 US presidential election, and the threat of similar interference with the mid-term election on 6 November 2018. The challenge facing Western governments was highlighted on 27 July, when Facebook's then chief security officer (CSO) Alex Stamos stated that he believed it was too late to prevent Russian interference in the mid-terms.

Microsoft had already announced on 21 August that Russian hacking group Strontium – also known as Fancy Bear or APT28, among other pseudonyms, and identified in Mueller's July indictment as responsible for the 2016 election interference – had attacked the websites of US political parties, politicians, and news outlets.

Overt response options

The implementation of economic sanctions by a number of Western governments, targeted visa refusals, the expulsion of suspected intelligence operatives from diplomatic positions, strategic communications campaigns, and the threat of legal proceedings have formed the backbone of the overt Western response to date. In the UK, this has included action against Russian 'dirty money',

with measures such as Unexplained Wealth Orders being proposed to induce compliant behaviour among Russian oligarchs with UK financial interests.

[Continued in full version…]

(1075 of 5081 words)

For the full version and more content: