BEHIND THE ENIGMA: THE AUTHORIZED HISTORY OF GCHQ, BRITAIN'S SECRET CYBER-INTELLIGENCE AGENCY

Date: November 24th, 2020

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 24th, 2020, Professor John Ferris presented *Behind the Enigma: The Authorized History of GCHQ, Britain's Secret Cyber-Intelligence Agency* at the 2020 CASIS West Coast Security Conference. The presentation was followed by a question and answer period.

NATURE OF DISCUSSION

Presentation

Professor John Ferris' presentation focused on the history of signals intelligence (SIGINT) and its development from the First World War until today, and the security implications of SIGINT in the modern era.

Question and Answer Period

The question and answer period focused on the increased use of the internet by extremist actors and the implications for SIGINT agencies, and the evolving relationships between the SIGINT agencies of Western countries.

BACKGROUND

Presentation

The information that is provided during this talk is sourced from the research that John Ferris conducted for his book, *Behind the Enigma: The Authorized History of GCHQ, Britain's Secret Cyber-Intelligence Agency*. None of the information that is presented within the talk is classified and is freely available to the public. Within the next five years even more will be revealed about the history of

SIGINT, especially with concern to the Cold War, as some Western governments declassify more documents from that era.

Modern signals intelligence (SIGINT) began in 1914 in the context of WWI. This new form of intelligence involved the interception of signals, breaking of encryption, and the ability to discern actionable information from the intelligence collected. These intelligence processes were enabled during WWI by the rise of electronic communication by radio waves. In the First World War, every major power on both sides of the war that had the ability to conduct SIGINT did it. By 1915, the British had begun to implement the bulk collection of SIGINT and analysis of this intelligence. The SIGINT capabilities of both the Allies and the Central powers were relatively balanced during WWI. Following WWI, every major power maintained and expanded their SIGINT agencies, however, the number of people working in these agencies - numbering in the 1,000s per country - remained small compared to modern standards.

When WWII broke out, the SIGINT capabilities of all of the belligerents was highly capable - including the Axis powers. However, from around 1942 onwards the Allies gained the upper hand with the use of computing power, which ushered a new era of SIGINT. This upper hand was proven when Alan Turing and his team managed to crack the German Enigma code. Although SIGINT can contribute greatly to the success of a wartime effort, it is not the only key to success.

Following WWII, major governments were convinced that SIGINT was a vital component of national defense, and during the Cold War SIGINT agencies among major powers grew substantially with the number of workers in this field reaching the 100,000s by the 1990s. SIGINT became more permanent and powerful than ever as international alliances were formed between sub-national SIGINT agencies including the Five Eyes (Canada, Britain, Australia, New Zealand, and United States of America) and among the Warsaw Pact countries. SIGINT, during the Cold War was largely a state versus state matter with the exception of civilian and satellite radio which was collected and largely thrown out because it was not deemed to be important during the Cold War.

The rise of the internet changed everything. SIGINT changed from a largely state versus state issue into a state and society issue. The walls between foreign and internal communications started to dissolve as militaries and governments began to communicate over the same systems as civilians. The number of actors within the SIGINT space has now expanded greatly with governments, firms, and private citizens now being able to engage in SIGINT activities as it has become

a vital part of many people's everyday lives. This has made an increasing amount of institutions and individuals vulnerable. Bulk collection of information by government SIGINT agencies is necessary to protect against threats. Likewise, the communications of most citizens are largely discarded. Unilateral disarmament of these capabilities in the West would only make those countries vulnerable to adversaries such as Russia and China.

Question and Answer Period

The rise in the use of the internet by extremist groups raises concerns about the intersection between traditional SIGINT conducted by agencies on foreign communications and internal communications conducted by British, Canadian, and American citizens. Therefore, this area presents many legal complications for these agencies. A possible dilemma is that these are such important modes of communication and are so routinely used that one has to assume that some of the targets are using it. A new means of collecting what is now called SOCMINT or social media intelligence can help translate old practices of SIGINT into new media. However, whatever one can come up with is a set of approaches that all instinctively conflict with the privacy of some individuals. Personally, John Ferris is not concerned with what Five Eyes agencies are doing with their work on these issues for one simple reason: their resources are so limited that it's actually almost impossible for them to do many bad things. However, it will require a great amount of engagement with the public to resolve concerns about privacy infringement.

Historically, insular intelligence alliances like the Five Eyes, inhibited other countries from gaining access to important SIGINT. For example, SIGINT sharing between Five Eyes countries and NATO partners was dysfunctional for years. After 9/11, there has been increased sharing between SIGINT agencies in Western nations, however, intelligence sharing between these countries will always face political problems.

KEY POINTS OF DISCUSSION

Presentation

- Modern SIGINT began during WWI with the advent of radio wave communication.
- During the interwar period all major powers maintained and increased their SIGINT capabilities.

- Both sides of WWII were capable in the area of SIGINT, however, the allies gained the upper hand with the use of computer technology.
- During the Cold War there was a large expansion of SIGINT agencies and the creation of intelligence alliances like the Five Eyes.
- The internet changed everything with private citizens now communicating with the same systems as governments and militaries, and SIGINT has now become part of our everyday lives.

Question and Answer Period

- The rise in the use of the internet by extremist groups raises concerns about the intersection between traditional SIGINT conducted by agencies on foreign communications and internal communications. Continued engagement with the public to resolve concerns about privacy infringement is required.
- Insular intelligence alliances have and will continue to inhibit the sharing of SIGINT intelligence.

SFU LIBRARY DIGITAL PUBLISHING