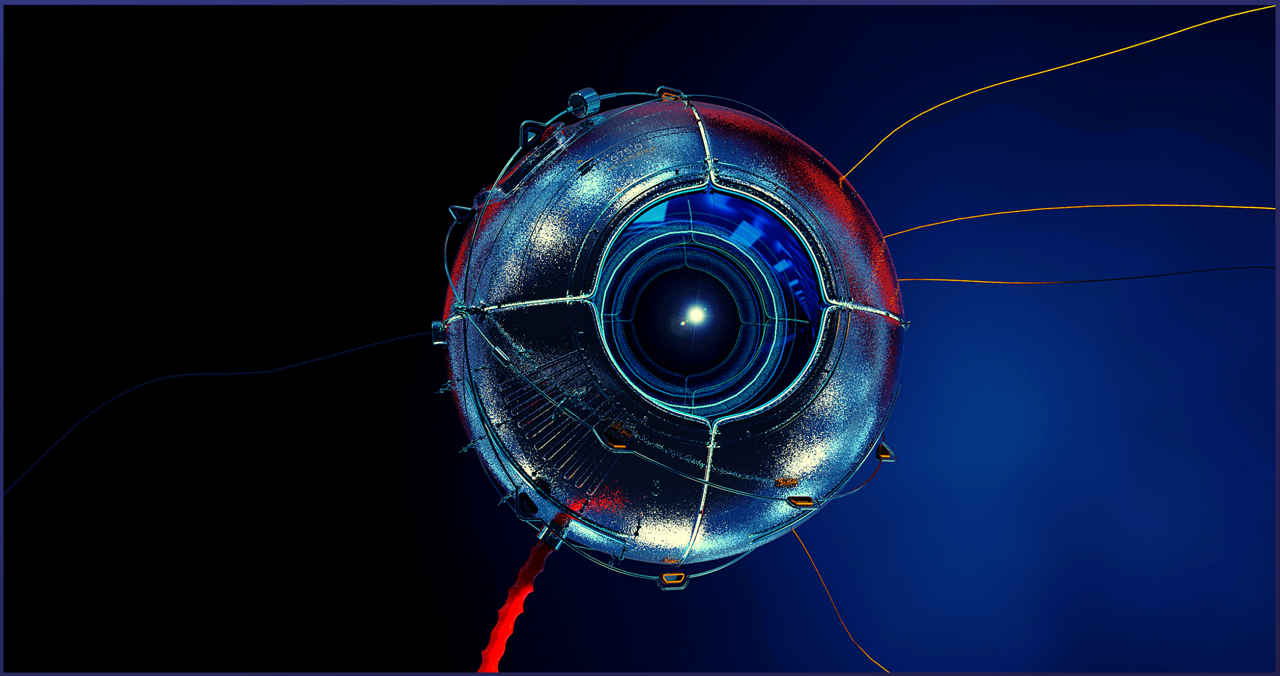
# Cyber Espionage

Conference Report
2nd-3rd May 2019

Centres for Doctoral Training in Cyber Security:

University of Oxford &
Royal Holloway, University of London



# Contents

EPSRC
Pioneering research and skills

UNIVERSITY OF OXFORD

ROYAL HOLLOWAY UNIVERSITY OF LONDON

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

# Why Cyber Espionage?

Cyber espionage is an increasingly pertinent topic of attention in UK news, amongst security researchers, and within intelligence communities. Historically, spaces like Bletchley Park have framed intelligence and counterintelligence operations as interdisciplinary activities, and this is a perspective that was echoed by our cyber espionage conference at University of Oxford.

The 5th annual conference was organised and run by a committee of Oxford and Royal Holloway doctoral researchers studying at EPSRC Centres for Doctoral Training, all of whom come from different discipline backgrounds, but were inspired to come together with the aim of contributing to a better cyber security future for the UK.

As adversaries with evolving technological toolkits continue to mount novel attacks to undermine UK's security, surveying current cyber espionage capabilities has potentially never been more pressing.

This report on the event summarises each speaker's conference presentation*, and is intended to contribute to a discussion about UK security and also the international discussion on how cyber security and cyber espionage will advance in the 21st century.

*Each talk is the editors' summary and may not represent the totality of each speaker's point of view

# '*The Universities-Security-Intelligence Nexus'*:
# Liam Gearon, University of Oxford

## *“What Does Secret Knowledge Achieve?”*

The triad of universities, security (*military*) forces, and intelligence communities form a nexus of knowledge exchange that has existed for decades. Gearon's talk articulated the details of this relationship, and drew on his forthcoming publication '*The Routledge International Handbook of Universities, Security and Intelligence Studies'*

Two individuals who have demonstrated how these three worlds overlap, are: Dwight Eisenhower, who served as Army General in the US military, as 34th US President, and as 13th President of Columbia University; and former FBI Director James Comey, the latter of whom co-hosted an invite-only student cyber security conference at Boston College in 2017

Security after World War Two expanded from the domain of the military to something now also studied and conceptually contributed to by academics - a phenomenon of militarisation, perhaps, evidenced by the existence of our own conference.

The university campus is no stranger to the world of espionage, a contemporary example being foreign students and foreign professors monitored by intelligence communities for fear of industrial or state espionage.

Universities are a complicit actor in the intelligence-security apparatus. At times, universities have been the bedrock of anti-government critique, or have cemented the power of intelligence communities. Perceived as liberal institutions, universities may portray their relationship with intelligence and security agencies as somewhat more distant than what Gearon would say is the reality.

Collaborative research between these spheres is important for securing peace, but the role of the academic must be viewed as tied to the security-intelligence world. This realisation comes with ethical issues, as the knowledge shared by universities can contribute to military activities that may result in the death of adversaries and possibly even civilians.

Our first speaker set the stage for us to consider what it means for us to be security researchers, reminding us that it is not a responsibility to be taken lightly.

# *'Open Source Intelligence':*
# Niamh Healy, Ridgeway Information

*“Open Source Information is Potentially More Verifiable”*

Open source intelligence (OSINT) communities are a different and less well-established kind of intelligence group. Healy emphasised the role of OSINT in verifying the commitments made by states to nuclear nonproliferation, for example. OSINT thus maintains an international peacetime status quo that avoids kinetic escalation (*physical retaliation*).

There are several examples of civilian OSINT being used to supplement state-sanctioned cyber espionage, notably Bellingcat’s unmasking of the GRU operatives (allegedly) responsible for the Skripal poisoning, but also situations in which using publicly available satellite imagery has facilitated the identification of cases of Chinese industrial espionage.

The use of OSINT to avoid states having to call each other out for international norms violations allows civilians to do what was previously the remit of media (to whom spies leaked their findings).

Now, OSINT communities can corroborate each other’s work and actively shape global relations, without causing international tensions or endangering human espionage operatives.

OSINT also highlights the imperative to approach intelligence gathering from a variety of cultural and linguistic perspectives. The ability to translate information from and into various languages is an asset to all intelligence communities; it is a telling geopolitical picture that GCHQ advertise jobs for speakers of Russian, Farsi, Mandarin, and Arabic.

# *'Cyber Espionage in Law and Policy':*
# Robert Carolina, Royal Holloway, University of London

## *“Cyber Espionage is a New Tool in an Old Game”*

The spectres of China, Russia and North Korea loomed large during Carolina’s talk.

Cyber espionage is simply defined, with influence from NATO’s Tallinn Manual, as 'information gathering via cyber capacities'. Cyber espionage as a tool is indispensable, as it gives adversaries a cheap method to gather large amounts of data and influence other states, all without fear of potential reprisal as the veil of anonymity can obfuscate actions and identity.

Legally, ‘cyberspace’ does not exist. International law is such that cyber operations and espionage can violate the sovereignty of a State, and prosecution and penalties are both dependent on the physical location of the attackers and their targets.

However, attribution of adversaries’ activities is hard, and the question becomes how one can legally designate the responsibility of an action. Is a State ‘responsible’ if one of its citizen carries out a cyber operation against another State?

Yes, the State is able to convict the attacker under their own domestic laws, but the State that houses this individual is not necessarily seen as a complicit actor.

A non-state actor’s cyber-operation, when directed by the State, can become attributable to the State, and therefore are an issue for international law. Cyber attacks *are* prohibited by international law: one cannot injure a person or damage objects via a cyber operation. Still, cyber espionage, *per se,* is not actually a violation of international law, but the methods for conducting cyber espionage may violate laws and agreements.

Although espionage has existed for centuries, the prefix of ‘cyber’ multiplies the complexities that the UK must navigate in the 21st century if we are to withstand adversaries’ information-gathering attempts, and launch our own.

# *'Gender and IoT'*
# Leonie Tanczer, University College London

## *“Intimate Espionage; Spying within the Home”*

Security threats are usually conceptualised by most to be at State-level. Tanczer highlighted that some cyber security threats are on the scale of the household, but are still very much existential.

A very different notion of ‘cyber security’ is enacted, whereby devices and the control over them are used to undermine an individual’s privacy and security on a daily basis. This is ‘technology-facilitated abuse’. As the Internet of Things (IoT) expands, an increasing number of devices in our home and on our body will convey instantaneous data.

These devices can be weaponised by anyone to facilitate surveillance, control, and abuse. Tanczer stated that this abuse is highly gendered, with the purchase, set-up, and maintenance of domestic technologies often carried out by men, leaving women in situations whereby their devices (and their lives) are at the mercy of their partners.

We participated in a live experiment to investigate the vast array of ‘spying’ apps. We found apps - sold as parental monitoring for children’s phones, which is problematic in itself - that could be downloaded to become a digital panoptic surveillance system for an abused person if downloaded onto their phone by a partner.

This app would give the controller complete access to GPS location information, call data, message content, live listening capabilities, and access to Internet history and picture memory.

Tanczer and her research partners run workshops working with survivors of such abuse and their social workers, arming them with the information they need to stay safe and to realise when abuse is taking place.

Ultimately, however, police services and policymakers need to give technology-facilitated abuse closer attention, with a legal emphasis on how taking control of devices can contravene someone’s rights - even if it is a partner committing this crime.

## *'Cyber Intelligence and Offensive Operations'*
## Stephen Wolthusen, Royal Holloway, University of London

### *“From Port to Porch”*

This session was based around the technical controls and tools that can be used to implement different forms of intelligence gathering from “inside the system”.

For all its perks, the Information Age has caused many issues for the signals intelligence community as there is simply too much data to be comprehensively analysed. This situation will only get worse - it is speculated that by 2022 there will be over 122 Exabytes of data communicated over the Internet per month.

In addition to this, the deployment of cryptographic protocols across devices at all layers of society makes interception and analysis of electronic communications more difficult.

Wolthusen suggested that to negate this, intelligence agencies (and wannabe spies) are resorting to compromising devices at a hardware level or network level, where less verification occurs.Spying in this manner can have the benefit of not interfering with the target, which for some industrial systems is vital.

There is also the benefit of additional contextual information by eavesdropping at the endpoints of the communication versus intercepting messages in transit.

This is often enacted through supply chain attacks. Indeed, most hardware developers have been forced to outsource the production of the hardware to a third party due to the exorbitant costs of manufacture. This immediately places control of the supply chain and verification of hardware with an external organisation, which may not be ideal.

This risk is well-known; the NSA produced their own computer chips at Fort Meadle to prevent this sort of attack. However, the economic and market factors associated with such a decision ultimately prevented this from being a viable long-term strategy.

Suggested solutions include verification of computer systems at all levels, built around secure tools and services. This is especially important due to the incredible difficulty of verifying components at circuit-level.

# *'Operational considerations'*
# David Pickard, Independent security researcher

## *“The Reality of Cyber Espionage”*

For all of the theory discussed so far, cyber espionage is still a new and changing field. Pickard highlighted that, for British intelligence agencies, intent is key -  namely, 'why is the operation being carried out?' The associated costs, qualities, and results are all important aspects to consider when deciding which counterespionage approach to deploy.

The contrast between human intelligence and signals intelligence was also discussed at length - both in terms of personnel that are needed to carry out the operations, but also in terms of the information that is to be extracted.

Cyber security uniquely sits between these two realms - as opposed to traditional signals intelligence (which is mostly passive) and to human intelligence (which can be very direct). Ultimately, however, cyber espionage must be used carefully due to the plethora of data available and the lack of resources that so often characterises cyber operations.

Public perception of cyber capabilities can also impact the choices on when and how to use certain cyber espionage techniques - as is often the case, they may be widely perceived positively or negatively, depending on the scenario and current affairs.

In addition, Pickard mentioned the difficulty of cross-border information sharing. The tension between the increasing internationalisation of intelligence and data protection regulation can cause conflict while conducting effective and safe espionage operations.

Even in our domestic setting, Pickard highlighted how UK legislation restrains and guides the behaviour of members of our intelligence agencies. The politics of a warrant request and warrant-signing, for example, were mentioned as crucial for keeping surveillance at an ethical level - preventing undemocractic mass ‘surveillance’.

# *CDT PhD Students' Lightning Talks*

The goal of this session was to allow doctoral students to discuss relevant topics of interest

To begin, Amy Ertan informed the audience about the lack of consensus surrounding the term “algorithmic warfare” in current research literature.

Following this, Freddie Barr-Smith discussed the art of penetration testing and using it to assess aspects of an organization’s security policy and culture.

Dray Agha then examined how information and territory are utilised and weaponised in contemporary Russian military doctrine.

Finally, Fatima Zahrah and Julia Slupska detailed their systematic approach of applying the “pathetic red dot theory” to the issue of tech-facilitated domestic abuse.

# Summary

One theme that influenced all of the talks was the rule of law: how the stipulations of legislation and regulation determine what actions institutions can and cannot undertake; how policy and policymakers with a global outlook have inherited a mosaic of national laws that conflict and run parallel to one another; how these issues make international legal collaboration difficult between States; and also how government policy needs input from industry and academia.

The UK, and its allies, are currently grappling with whose technology they can trust: the concerns over Huawei, and if they are an honest global telecommunications corporation, or a mechanism for the Chinese state to commit cyber espionage on a global scale. The potential for an adversary to have unhindered access to telecommunications is a grave threat worth investigating by all disciplines and communities.

Now, more than ever, research is needed to inform policymakers' decisions on what and whose technologies should be legislated for and against. Research is needed into how technology can be exploited in unexpected ways, making material threats that could not have been conceived. Research is also needed in the 'attribution' problem, to better discern who exactly the adversary of a cyber operation is, so they can face legal and economic repercussion.

Research in espionage is difficult, given that much remains privy to government institutions only. But difficult is not impossible. It is up to us all to proactively contribute to our nation’s security and to foster international relations to guarantee that future policies and laws will be crafted within the context of a global community centred around the values of freedom, democracy, and equality.

# Contact the Organizers and Editors

UNIVERSITY OF
OXFORD

CENTRE FOR
DOCTORAL TRAINING
in CYBER SECURITY

ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

**Anjuli Shere**
Anjuli.Shere@new.ox.ac.uk

**Hayyu Imanda**
Hayyu.Imanda@exeter.ox.ac.uk

**Joe Rowell**
Joe.Rowell.2015@live.rhul.ac.uk

**Dray Agha**
Dray.Agha.2014@live.rhul.ac.uk