Applicant: **Whyte, Jeffrey**
Organisation: **University of Manchester**
Funding Sought: [redacted]

[redacted]

PRIMARY APPLICANT DETAILS

Title	Mr
Name	Jeffrey
Surname	Whyte
Tel (Work)	[redacted]
Email (Work)	[redacted]
Address	Oxford Road Manchester M13 9PL United Kingdom

CO-APPLICANT DETAILS

Title	Professor
Name	Maja
Surname	Zehfuss
Tel (Work)	[redacted]
	[redacted]
	[redacted]
Address	Oxford Road Manchester Lancashire M13 9PL United Kingdom

CONTRIBUTOR DETAILS

Role	**Nominated Referee 2**
Title	Dr
Name	Victoria
Surname	Basham
Organisation	Cardiff University
	[redacted]
	[redacted]
	International Relations Museum Avenue Cardiff CF10 3AX United Kingdom

Role	**Research Support**
Title	Mr
Name	Neil
Surname	Chetham
Organisation	University of Manchester
Tel (Work)	[redacted]
	[redacted]
Address	Oxford Road Manchester M13 9PL United Kingdom

Role: Nominated Referee 1

Title: Professor
Name: Robert
Surname: Geiser
[redacted]
Email (Work): [redacted]
[redacted]

430 Science Hall , 550 N. Park St
Madison
Dane
53726
United States

Role: Head of Department

Title: Professor
Name: David
Surname: Richards
Tel (Work): [redacted]
[redacted]

Address: Oxford Road
Manchester
M13 9PL
United Kingdom

Role: Current Supervisor

Title: Professor
Name: Derek
Surname: Gregory
[redacted]
[redacted]

Address: Peter Wall Institute of Advanced Studies
6331 Crescent Road
Vancouver
British Columbia
V6T 1Z2
Canada

Section 1 - Eligibility Criteria

Please confirm whether you meet the eligibility criteria for the Newton International Fellowship Programme as follows:

Do you hold UK Citizenship?

⊙ No

Do you hold a PhD?

⊙ No

When do you expect to be awarded your PhD?

30 April 2019

Do you have between 0 to 7 years of research experience since your PhD (factoring in career breaks and/or part-time working)?

⊙ No

Are you proficient in reading, writing and speaking English?

⊙ Yes

Section 2 - Contact Details

PRIMARY APPLICANT DETAILS

Title	Mr
Name	Jeffrey
Surname	Whyte
Tel (Work)	[redacted]
[redacted]	[redacted]
Address	Oxford Road Manchester M13 9PL United Kingdom

CO-APPLICANT DETAILS

Role	Research Support
Title	Mr
Name	Neil
Surname	Cheetham
Organisation	University of Manchester
Address:	Oxford Road Manchester M13 9PL United Kingdom

Role	Head of Department
Title	Professor
Name	David
Surname	Richards
Address:	Oxford Road Manchester M13 9PL United Kingdom

[redacted] [redacted]

[redacted] [redacted] [redacted]

Type: University

Name: Cardiff University

[redacted] [redacted]

Address: Cardiff University
Cardiff
Cardiff
CF10 3AT
United Kingdom

up to three if applicable.

up to three if applicable.

No Response

up to three if applicable.

No Response

No Response

Summary

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Section 5 - Research Proposal

Primary Subject

Please indicate the subject most relevant to your research:

Politics

Project Title

Constructing Insecurity in the Age of Disinformation

Start Date

01 October 2019

End Date

01 October 2021

Proposed Host Institution

Please indicate here your choice of host institution, including the appropriate Faculty, Department, Research Institute or College where you propose to work:

University of Manchester, Department of Politics, School of Social Sciences, Faculty of the Humanities

Reason(s) for choice of host institution

Please explain the reason(s) for your choice of UK host institution (the university/research institute, department):

Manchester is a top ten ranked University for Politics in the UK. The priorities of the department's research clusters closely align with those of my proposed research. The department's 'Critical Global Politics' cluster specializes in research on the politics of knowledge, news and media, the role of technology in securitization, and most importantly cyberwarfare. The department's 'Comparative Public Policy and Institutions' cluster will help refine my approach to studying cybersecurity policies as they continue to roll out internationally. In the 'Global Political Economy' cluster I will find colleagues interested in the intersection of problems concerning the privatization of security services and the increased concentration of media firms that have contributed to the contemporary crisis of disinformation and cyber-insecurity. Particularly, I am interested in supplementing my current expertise in historical, archival, and qualitative methodologies through training opportunities at Manchester's Cathie Marsh Institute, with its emphasis on interdisciplinary and quantitative methodologies.

Abstract

Once a relic of the Cold War, 'psychological warfare' has returned to the public spotlight in the wake of the 2016 Brexit referendum and American presidential election. Purportedly facilitated by sophisticated online 'cyberwarfare' activities, the new hybrid cyber-psychological warfare has produced what many have identified as a 'post-truth era' in which socially mediated disinformation presents threats to democracy and election integrity. This project proposes to study the rise of the cybersecurity industry, its role in the construction of elections as new objects of security policy, and the broader threat of 'cyber insecurity' as such. Drawing upon the applicant's research on the history of American psychological warfare in the 20th century, this project seeks to interrogate the construction of the current 'propaganda scare' and consider the extent to which popular framings of foreign 'information threats' are being leveraged to justify new rounds of securitization and military spending.

This project revolves around identifying cybersecurity's networks of consolidation between government, industry, and the academy, and its networks of dissemination between journalists, think tanks and advocacy groups. Fieldwork for this project will consist of attendance at cybersecurity conferences where government, industry and academics converge to define crises of cyber-in/security and propose political, military, and commercial solutions. This project takes a mixed method approach to producing qualitative and quantitative datasets. In addition to qualitative analysis of these events and their themes, this project will yield social network data and analysis concerning the proliferation of the professionals and organizations driving the contemporary movement toward the securitization of information and knowledge. In addition to mapping the social and professional contours of these inward-facing networks of cybersecurity consolidation, the applicant will code and analyse popular cybersecurity discourse in order to map the contours of cybersecurity's construction in the press and media. This project's key contribution and impact lay in determining the extent to which the emergent cybersecurity industry has and continues to define the terms of political threat and crisis, and the extent to which these discourses serve the interest of the publics of both the UK and the applicant's home country of Canada.

Lay Summary

As narratives surrounding 'psychological' and 'cyber' warfare proliferate in the popular press, it has become increasingly common to refer to the present moment as a 'post-truth era' in which socially mediated disinformation threatens the integrity of democratic elections. With cyberwarfare specifically targeting online political discourse, publics have become increasingly reliant on experts to identify 'informational threats' and parse disinformation. Amidst calls for stricter gatekeeping from media firms, this project calls into question the role of the cybersecurity industry in exacerbating popular currents of mistrust. Drawing on the applicant's PhD research on the history of 'psychological warfare' and its longstanding relationship

with efforts to influence foreign elections, this project seeks to understand why emphasis on so-called 'psychological warfare' has dominated popular political discourse since 2016. To this end, this project seeks to identify the vested political and economic interests underwriting 'cybersecurity' and attempts to 'secure' political discourse and public opinion.

Research Proposal

⊙ PDF upload

Research Proposal

J Whyte — Proposal
16/03/2019
01:39:48
pdf 110.49 KB

Previous Contact

I have corresponded with the Co-applicant in planning and preparing this fellowship application, primarily through email and video-conferencing.

Training Programme

Within Manchester's department of Politics, this project has the supervisory support of Maja Zehfuss, whose work on post-structuralist theories of war emphasizes the contingent and constructed nature of narratives that frame threat, vulnerability, and the necessity of prosecuting war. Under the supervision of Dr. Zehfuss, I stand to benefit from her knowledge and theoretical perspective on warfare, the logic of security, and contemporary constructions of the 'necessity of cyberwarfare'. Dr. Zehfuss' mentorship will be invaluable for deepening my knowledge of the historical and political dimensions of my project from a humanities perspective. In particular, Dr. Zehfuss will be able to assist in the design and refinement of the qualitative classification scheme through which I intend to produce the project's datasets.

Crucially, a fellowship at Manchester will allow me to receive training in the quantitative research methods that will be vital for my project's success. As a political and historical geographer, it is in the area of quantitative methodology that the greatest contributions to my research potential can be made. To this end, I have discussed my project with Rachel Gibson, director of Manchester's Cathie Marsh Institute (CMI) for Social Research. Dr. Gibson has offered her support for this project, and will assist me in connecting with other relevant scholars at Manchester and further afield. Founded in 2014, the CMI is a world-class research center focused on the application of quantitative methods to interdisciplinary social science research. In terms or training, I stand to benefit most from the CMI's two training-oriented research groups: the Data, Skills, and Training group, and the Statistical Modelling Group (STMG). Both research groups provide a range of short courses, seminars, and workshops ranging from introductory to advanced level instruction on quantitative methodology design, data analysis, and software training.

In partnership with the Cathie Marsh Institute, Manchester also offers numerous opportunities for training through its university-wide methods@manchester initiative, as well as offerings through the National Center for Research Methods. Upon arriving at Manchester, I intend to enroll in several seminars and short courses to grow the methodological scope of project through statistical and data literacy, such as 'Introduction to Data Analysis', 'Practical Skills for Data Analysis', 'Social Media for Data Analysis', and 'Introduction to "R"', a popular statistical analysis language. Specifically, the CMI's Statistical Modelling Group offers short courses directly related to my project methodology of social network analysis: 'Multilevel Analysis of Social Network Data' and 'Nvivo for Qualitative Data Analysis'. The latter course will also offer instruction in designing research involving coding methodologies. A fellowship at Manchester is therefore a

unique opportunity to expand the scope of my methodological approach, and to undertake research that will produces datasets valuable to other scholars and researchers.

Benefits to individuals/institution

My project contributes to the core research themes of Manchester's department of Politics. To the department's 'Critical Global Politics' cluster, my project speaks to questions concerning news and media, cyberwarfare, the role of technology in securitization, and the politics of knowledge. To the 'Comparative Public Policy and Institutions' cluster my project contributes research on rhetoric and public policy concerning cybersecurity and current efforts to solidify policy concerning it. Here my project is supported by Nick Turnbull, whose work on political rhetoric will contribute to my understanding of cyberwarfare's popular construction. To the 'Global Political Economy' cluster, my project contributes an interrogation of cybersecurity in relation to broader structures of military-industrialism, and to its specificity in constructing the 'post-truth era' crisis. Here my project has the support of James Pattison, whose work on Private Military Contractors (PMCs) will help inform my political economic approach. Finally, my project's engagement with electoral politics as primary cyberwar targets speaks clearly to the department's Democracy and Elections cluster, and has the endorsement of the cluster's convenor, Rachel Gibson. My project also has the support of Emma Barrett, convenor of the Cathie Marsh Institute's Privacy, Data Protection, and Trust research group.

Benefits to Overseas Country

According to Canada's Financial Post, Canadian businesses spent over $14 billion on cybersecurity services in 2017. In response, the Canadian federal government announced the establishment of a Canadian Centre for Cybersecurity in February of 2018, with plans for the centre to be fully operational by Spring of 2020. The government's plan emphasizes collaboration between government and industry, promising that the Centre will be 'a single unified source of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public.' To support the effort, the Canadian government has published an 'Introduction to the Cyber Threat Environment' which identifies a range of cyber-threats scales and sources, from the geopolitical at the national scale, to terrorism at the local and individual scale. As national cybersecurity policies and budgets roll out in real time, my project's concern with tracking the advocacy networks and political economy of cybersecurity is a timely contribution to knowledge relevant to Canada's public interest.

Benefits to UK

As controversies continue to swirl around the role of cyberwarfare and online influence in the 2016 Brexit referendum, the UK has also established a National Cyber Security Centre, which became operational in October of 2016 under the direction of the Government Communications Headquarters (GCHQ). British academic research since 2016 has become closely concerned with issues of cybersecurity and election integrity, as evidenced by the concerns of the British Election Study and the Engineering and Physical Sciences Research Council's (EPSRC) recent Trust, Identity, Privacy and Security (TIPS) research initiative. While my project takes seriously the threat of cybercrime and cyberwarfare, it also seeks to interrogate the political, economic, and rhetorical contours of the way in which cyber-in/security is constructed in both popular and professional circles. As government policy and spending formalizes around this new object of security, understanding the political landscape on which cybersecurity unfolds becomes a matter of intense importance to the British public and to British researchers.

Outline of Data Management and Data Sharing Plan

My project will produce quantitative datasets that support my observations concerning the social and rhetorical networks involved in constructing cybersecurity as a new object of policy. I will work closely with the Cathie Marsh Institute's Data, Skills and Training Research Group to make my data sets publically available for other researchers. To reach a wider lay audience, I will visualize data for popular impact, make

myself and my research available to journalists. I will pursue opportunities to publish editorials and columns in outlets like openDemocracy and The Conversation that can challenge and balance popular narratives that emphasize threat, insecurity and geopolitical conflict.

Additionally, I propose standard dissemination to the academic community through peer review. By the end of this fellowship's first year, I intend to prepare the findings of my initial review of cyberwar/security literature for submission to the European Journal of International Relations or Political Geography. In the fellowship's second year I intend to submit for publication two articles on the findings of my research into cybersecurity's networks of consolidation and dissemination, respectively. By the fellowship's end, I intend to have completed initial preparation for a monograph on the political contours of the cybersecurity landscape.

Overseas Field Research

⊙ Yes

Overseas Field Research

Whyte — Fieldwork
02/03/2019
23:17:07
pdf 15.31 KB

Section 6 - Use of Animals in Research

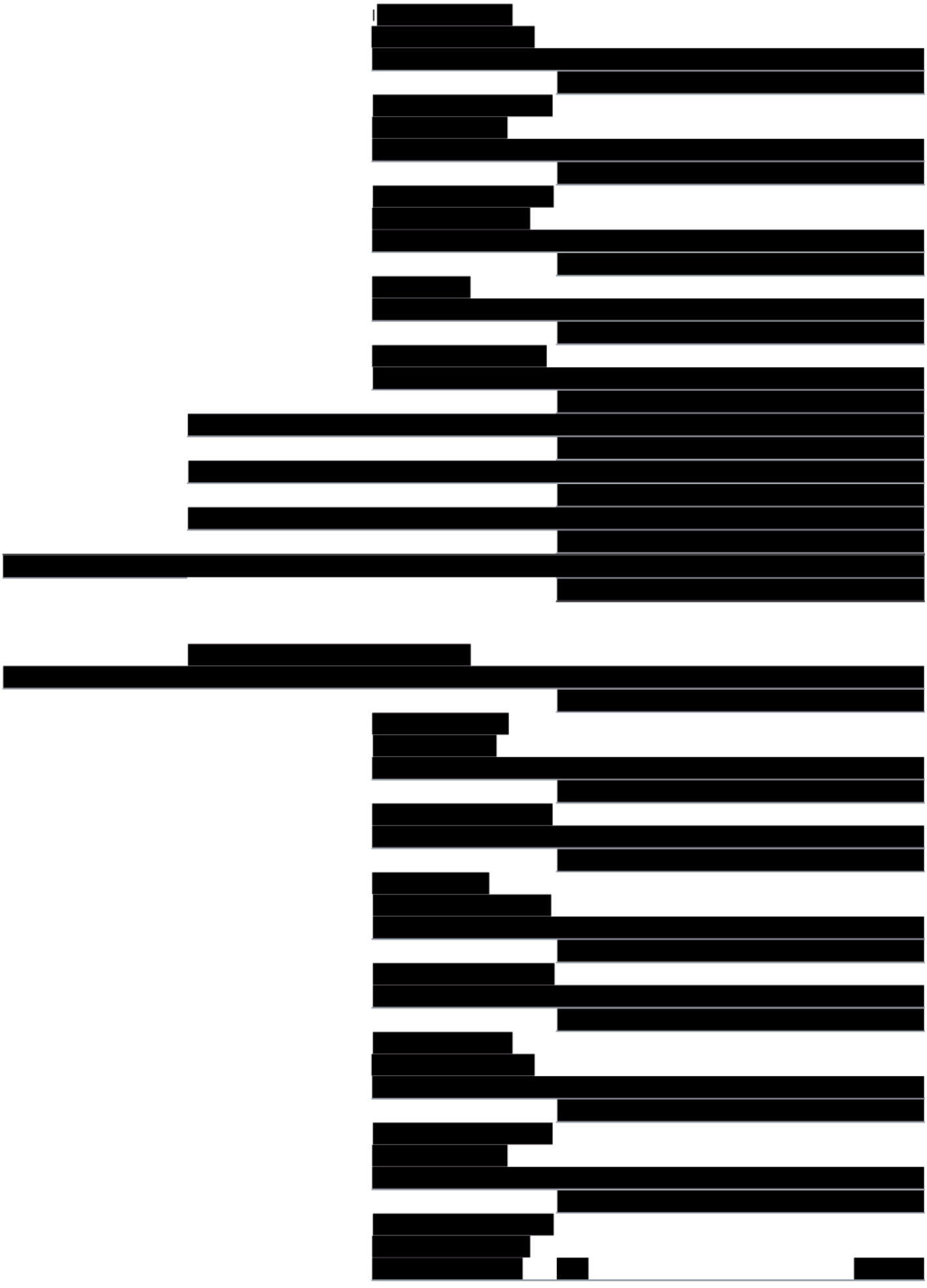
Does your proposal involve the use of animals or animal tissue?

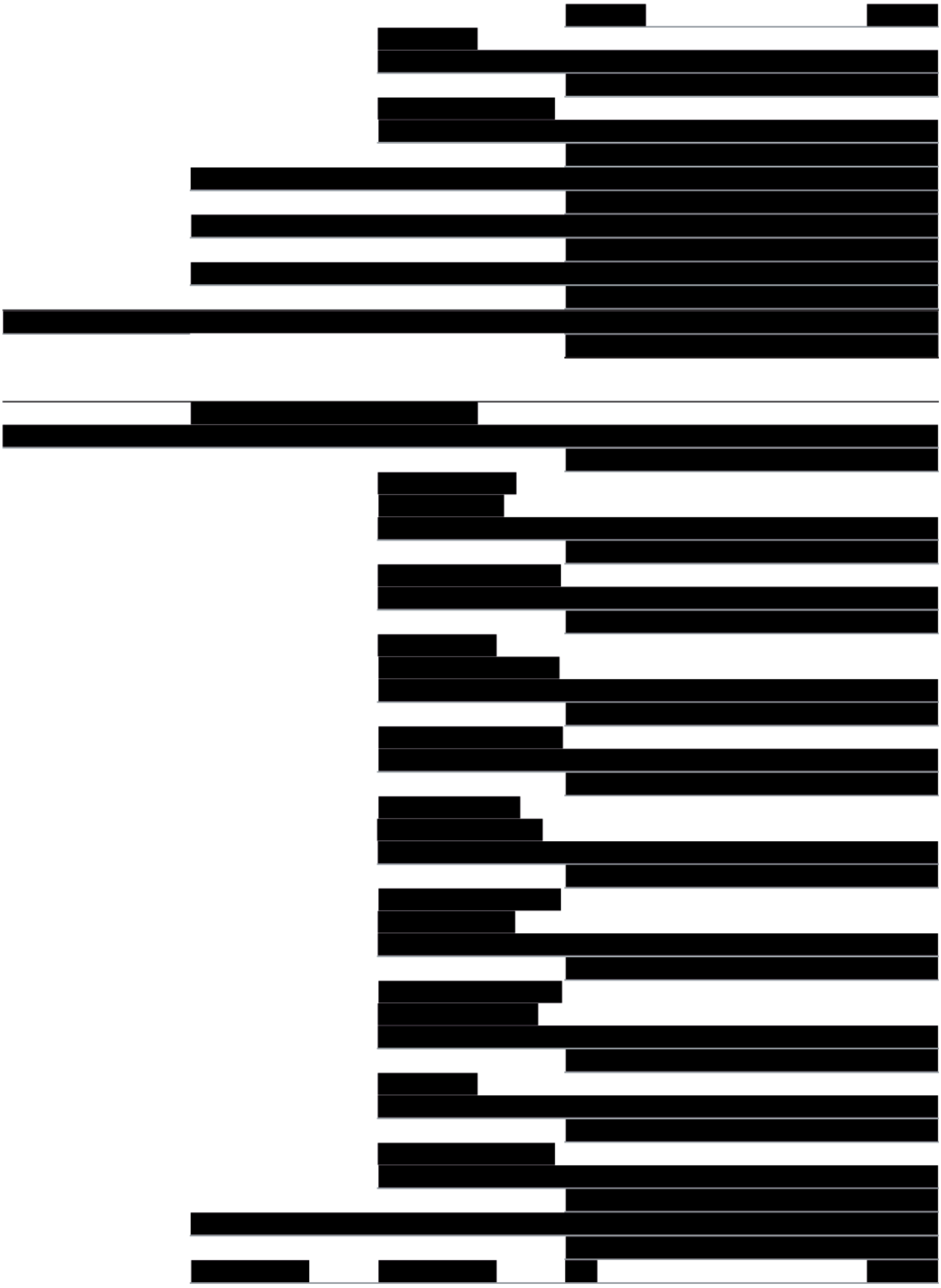
⊙ No

Section 7 - Financial Details

Please define the proposed budget for your project in the table below:

Period Group	Item Type	Item	Field	£
[redacted]				





[redacted]

Justification for Research Expenses

Fieldwork for this project revolves around attendance at international cybersecurity and cyberwarfare conferences. I will attend these conferences in a fieldwork research capacity, not to disseminate research, and therefore request consumables fieldwork expenses as outlined below. Cost estimates are based on the location and dates of this year's cybersecurity conference circuit. Final costs will be determined when the proposed conference locations are announced, and I will alter research plans as necessary to keep expenses within the proposed budget.

As I propose to attend the following conferences in both year 1 and year 2., total costs above represented a doubling of the following figures:

Cyber Defense and Network Security Conference-London

Return Train to London Euston £116
Accomodation for 3 nights @ £120/night
Subsistence for 3 days @ £30/day

Cyber Threat Intelligence Symposium-London

Return Train to London Euston £116
Accomodation for 3 nights @ £120/night
Subsistence for 3 days @ £30/day

Cybersecurity X Manchester Conference-Manchester

Local Travel @ £10/day
Accomodation 0
Subsistence for 3 days @ £30/day

Cyberwarfare Symposium- New York

Flight Return to New York £386
Accomodation for 5 nights @ £120/night
Subsistence for 5 days @ £40/day

InfoWarCon- Washington DC

Flight Return to Washington DC £541
Accomodation for 5 nights @ £120/night
Subsistence for 5 days @ £40/day

International Cyber Warfare and Security Conference-Turkey

Flight Return to Antalya £193

Accomodation for 5 nights @ £120/night
Subsistence for 5 days @ £30/day

European Conference on Cyber Warfare and Security-Portugal

Flight Return to Lisbon £155
Accomodation for 5 nights @ £120/night
Subsistence for 5 days @ £30/day

International Conference on Cyber Warfare and Security-South Africa

Flight Return to Durban £773
Accomodation for 5 nights @ £120/night
Subsistence for 5 days @ £40/day

Costs of £800 are request for conference registration fees.

Costs of £3000 are requested for relocation from current city of Vancouver, Canada in Year 1.

[redacted]

Section 8 - Applicant Declaration

Declaration

Checked

Applicant Name	Jeffrey Whyte
Date	24 March 2019

Professor Maja Zehfuss
Department of Politics
School of Social Sciences
The University of Manchester
Oxford Road
Manchester M13 9PL

maja.zehfuss@manchester.ac.uk
+44(0)161 275 4937
www.manchester.ac.uk

17 March 2019

Re: Jeffrey Whyte

Jeffrey Whyte's proposed research is timely, exciting and innovative. He is extremely well placed to undertake it and Manchester is able to provide a highly supportive environment for this research.

'Constructing Insecurity in the Age of Disinformation' proposes to think about current concerns over cybersecurity through the lens of psychological warfare. This is a potent connection. While concerns about foreign-steered propaganda and post-truth politics have reached fever pitch in liberal democracies, particularly around the potential for corruption of electoral processes, there has been less attention paid to how the reaction to these threats operates and how, crucially, this reaction itself changes the terms of engagement. There is no research I am aware of to date that links the practices of self-styled cybersecurity providers to conceptual questions about what kind of politics their practices promote. The increasing understanding of issues relating to new communication media as matters of security and indeed war invokes a particular politics, one in which nations states and democracies are at risk from outside interference. Thus, current concerns about isolationism, rising nativism and anti-migrant attitudes are then responses not (just) to the implications of outside interference but produced by the responses that are meant to protect us from these very problems. In short, Mr Whyte's proposal to investigate the politics involved in the production and dissemination of cybersecurity strategies is conceptually novel and intellectually fruitful.

Mr Whyte's doctoral research examines psychological warfare practices during the Cold War. This research, part of which has already been published in *Political Geography* and *Geopolitics*, shows him to be able to marshal a wide range of data from a variety of sources to make larger conceptual arguments. Thus, he is extremely well placed to undertake the proposed research. He has in-depth expertise on matters of psychological warfare, he is well versed in the literatures surrounding not just this topic but wider questions of politics and communication. Having read his published work in preparation for this application, I have come to realise how my thinking on the production of war as a cultural encounter could benefit from a deeper understanding on how its practices built on previous strategies for psychological warfare. The way in which public opinion is treated as a battlefield neither started with the cultural turn in warfare, nor has it ended with the increasing focus on apparently non-kinetic terrain (such as electoral interference). This ongoing history is, crucially, also central to current struggles over the (geo-)political imagination.

My own research is currently shifting from a concern with (traditional) war to one about the production of the 'migration crisis'. In this context, I am particularly keen to work with Mr

Whyte to develop my own understanding of post-truth politics and the significance of the currently radically contested nature of (geo-)political imaginaries. Having previously supervised a project involving the mapping of activities by private security entrepreneurs, I know how powerful such a detailed study can be to drive our understanding of bigger conceptual questions.

Manchester is able to provide an exceptional research environment for this thesis. We are proud of the wide range of training opportunities that we are able to provide, not least through methods@manchester. Expertise across a number of research clusters in the Department of Politics links to the proposed work, with work on war, security and the politics of truth in the Critical Global Politics cluster and work on the impact of new communication technologies on electoral politics in the Democracy and Elections cluster being the most obvious links. My colleague Rachel Gibson's expertise in the use, impact and politics of new communication technologies in relation crucially complements my approach to these questions.

We will provide support for Mr Whyte's career development through a process of discussion, reflection and support in the context of a personal development process. The areas that we have already identified in our discussions to date include: training in methods and approaches; support for the development of top quality academic publications; support and training for blog writing (e.g. through the opportunities offered by policy@manchester); and the broadening of his networks across relevant disciplines. The most crucial skill to learn during a postdoctoral project such as this is, in my experience, the ability to independently deal with the multiplicity of demands and identify appropriate priorities, balancing immediate pressures against long-term objectives. Thus, my aim would be for Mr Whyte to be not just well placed for the academic job market by the end of the fellowship, but to have the skills to navigate a successful career.

In sum, this is an outstanding and indeed urgent project, to be undertaken by an emerging scholar who has already proven his ability to develop significant new insights, which we would be excited to support.

Research Proposal

Once a relic of the Cold War, 'psychological warfare' has returned to the public spotlight in the wake of allegations concerning foreign and online interference in the Brexit referendum and American presidential election of 2016. Connected to concerns over 'cyberwarfare' and 'cybersecurity' (Kaiser 2015), this resurgence was most vividly illustrated in coverage of consulting firm Cambridge Analytica's so-called 'psychological warfare mindfuck tool'.[1] Prior to 2016, constructions of cybersecurity often focused on the protection of digital critical infrastructures like online banking platforms and electricity grids. Since 2016, however, 'cybersecurity' has increasingly come to denote the 'weaponization' of dis/information, and the 'securitization' of democratic elections and public opinion. This new hybrid of cyber- and psychological warfare has fomented political crisis and a so-called 'post-truth era' in the Anglo-American world. As one upcoming cybersecurity conference agenda makes clear, 'with the threat apparent, cyber operators from military and government are now faced by a new question: who, not what, will be targeted by hostile cyber operators?'[2]

Though popular coverage of the new cyber-psychological warfare often suggests frictionless manipulation by 'elaborate digital architectures' and 'sophisticated operations', questions of technology remain opaquely black-boxed. Consequently, professional organizations and security firms have been enlisted to evaluate and translate the digital esoterica of cyber-psychological warfare for lay audiences. My postdoctoral project proposes to study the rise of the cybersecurity industry and its construction of elections as new objects of security policy. While it is necessary to attempt to open up the black boxes of cyberwarfare technology, it is also crucial to understand how the black-boxing of cyber-psychological warfare becomes a geo/political strategy for framing political discourse itself, not as a process of democratic deliberation, but as an object of *security*. As cyber-psychological warfare becomes an increasingly common feature of the contemporary political landscape, how can scholars of security challenge state and private initiatives to 'secure' political discourse, while taking seriously the corrosive effect of online disinformation?

Approach

At the time of this writing, details are emerging that the UK Ministry of Defence's Defence Science and Technology Laboratory (DSTL) has offered UK universities £70 million for research on psychological warfare, 'information activities', and 'strategic communication'.[3] My project seeks to understand how popular framings of 'information insecurity' work to legitimize tighter relationships between the academy, government, and industry in the name of securitizing information against the 'post truth' malaise. My approach is informed by my doctoral and published research on the history of American psychological warfare in the 20th century (Whyte 2018b). Central to my work has been close analysis of the way in which 'foreign propaganda scares' have been constructed, used, and abused by parties seeking to influence public opinion. Orchestrated by the American intelligence community in the years prior to World War II, 'psychological warfare' first emerged as a term connoting the potency and apparent 'scientific' nature of German propaganda (Whyte 2018a). Though German propaganda had neither scientific basis nor purchase in the United States, its construction as such provided pretence for applying a militarized and securitized logic to the American press and public opinion. My approach and experience therefore provide a corrective to the current crisis by situating it within the longer history and structure of perennial 'foreign propaganda scares'.

---

[1] Cadwalladr, C. (2018). 'I made Steve Bannon's psychological warfare tool'. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

[2] Cyber Defense and Network Security Conference (2019). London: (https://cdans.iqpc.co.uk/).

[3] Gayle, D. (2019). 'UK military turns to universities to research psychological warfare'. *The Guardian.* https://www.theguardian.com/uk-news/2019/mar/13/uk-military-mod-universities-research-psychological-warfare-documents

More immediately, the new cyber-psychological warfare has emerged in the wake of the 21st century's 'cultural turn' in military affairs (Anderson, 2011; Belcher, 2012; Gregory, 2008; Zehfuss 2012). As Zehfuss (2013) has noted, military interest in staging war as a 'cultural encounter' has animated a liberal-humanitarian imaginary of war in which war itself is reduced to a problem of communication. In my PhD research I join critical scholars of war in showing that, far from providing alternatives to violence, so-called 'non-kinetic' and cultural strategies like psychological warfare have ultimately provide rationales for justifying and refining its use (Reid-Henry 2015; Weizman 2011). Though counterinsurgency warfare has fallen from favour in Western policy circles, the logic of warfare's 'cultural turn' persists in contemporary constructions of cyberwarfare. Just as narratives of 'humanitarianism' reduced war to a 'problem of communication', contemporary framing of cyber-psychological warfare now elevates questions of communication to the status of war. As narratives circulate constructing the spectre of a 'cyber Pearl Harbor', it is necessary to investigate and challenge contemporary efforts to transpose political discourse to the register of warfare and security.

Paradoxically, 'the politics of truth' in the 'post-truth' era have broadly elided overt questions of politics. In addition to assuming the existence of a bygone era in which matters of political truth were settled, the logic of 'securitizing truth' seeks to pose technical answers to political questions (Mitchell 2002). While warfare's 'cultural turn' was informed by the broader militarizaiton of the social sciences during the Cold War (Barnes & Farish 2006; Barnes 2008; Farish 2010; Solovey 2013), the contemporary 'cyber turn' is being underwritten by the authority of a new class of security experts positioning themselves, not so much as arbiters, but securitizers of truth. As appeals to authority for the securitisation of truth have defined the 'post-truth era', the American intelligence and security communities have undergone popular rehabilitation, and media monopolies like Facebook and Twitter have been called upon to assert stewardship over political discourse.

In place of these appeals, my project seeks to re-politicize the 'politics of truth', and to investigate the political landscape on which the securitization of truth unfolds. I draw upon my own research foundations to hypothesize both the concentration of media ownership and the rise of cybersecurity industries as correlates to contemporary currents of political mistrust and uncertainty. As firms like Cambridge Analytica advertise their incongruous ability both to influence *and* secure elections, it is necessary to interrogate the broader proliferation of cybersecurity 'intellectuals of statecraft' involved in constructing and tendering solutions to the apparent crisis. To this end, I hypothesize the existence of two distinct but interfacing networks: a network of *consolidation* between security contractors, governments, and militaries, and a network of *dissemination* between journalists, think tanks, and advocacy groups.

Methodology

My preliminary phase of research involves first a review of the rapidly proliferating literature — popular, academic, professional — on post-2016 cybersecurity and psychological warfare, and second, a series of semi-structured interviews with technological and quantitative researchers in both the UK and Canada.

To investigate cybersecurity's networks of *consolidation* per my fieldwork section, I propose attendance at major cybersecurity conferences at which professional, academic, and government actors gather to define questions of cyber-in/security. Through collection and recording of conference itineraries, literature, plenary addresses, and panel discussions, this research will yield new quantitative and qualitative data sets. Quantitatively, I will produce data on the affiliations of both individuals and organizations attending and sponsoring cybersecurity conferences to the end of mapping the social and professional networks invested in the construction of cybersecurity. Qualitatively, I propose an inductive classification schema of cybersecurity themes, topics, and tropes based on field observations. Once established, I will code conference content for subsequent mapping, analysis and comparison against my collected social network data.

To investigate cybersecurity's networks of *dissemination,* pursuant to my preliminary research I propose maintenance of an ongoing press file concerning its popular coverage by journalists, think tanks and advocacy groups. Analysis of this database will inform and be informed by my inductive classification scheme and provide further scope for scrutinizing points of contact between cybersecurity's networks of consolidation and dissemination. As a pilot study before this fellowship begins, I will attend a quintessential 'dissemination event' in Vancouver, Canada. Hosted by Simon Fraser University, the week-long 'community summit' titled 'Confronting the Disinformation Age' promises that 'together, we will co-create strategies to ensure stronger and healthier information ecosystems and stimulate more connected and resilient communities.'[4] A keynote panel forum for the event will be headlined by former George W. Bush speechwriter and 'axis of evil' architect David Frum (*The Atlantic*, American Enterprise Institute) and Cambridge Analytica whistle-blower Christopher Wylie, the latter of whose testimonies to U.S. Congress and UK Parliament have 'led to new legislative proposals in both countries.' This conference (April 10-18) will provide initial qualitative and quantitative data points, and allow me to refine my approach prior to undertaking further research.

Works Cited

Anderson, B. (2011). Population and affective perception: Biopolitics and anticipatory action in US counterinsurgency doctrine. *Antipode*, 43(2), 205–236.

Barnes, T. (2008). Geography's underworld: The military–industrial complex, mathematical modeling and the quantitative revolution. *Geoforum* 39(1):3–16

Barnes, T and Farish, M. (2006). Between regions: Science, militarism, and American geography from World War to Cold War. *Annals of the Association of American Geography* 96(4):807–826

Belcher, O. (2012). The best-laid schemes: Postcolonialism, military social science, and the making of US counterinsurgency doctrine, 1947–2009. *Antipode*, 44(1), 258–263.

Farish, M. (2010). *The contours of America's cold war*. University of Minnesota Press.

Gregory, D. (2008). 'The rush to the intimate': Counterinsurgency and the cultural turn. *Radical Philosophy*, 150(8).

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*, *46*, 11-20.

Mitchell, T. (2002). *Rule of experts: Egypt, techno-politics, modernity*. Univ of California Press.

Reid-Henry, S. M. (2015). Genealogies of liberal violence: human rights, state violence, and the police. *Environment and Planning D: Society and Space*, *33*(4), 626-641.

Solovey, M. (2013). *Shaky foundations: The politics-patronage-social science nexus in Cold War America*. Rutgers University Press.

Weizman, E. (2011). *The least of all possible evils: Humanitarian violence from Arendt to Gaza*. Verso Books.

Whyte, J. (2018a). "A new geography of defense": The birth of psychological warfare. *Political Geography*, *67*, 32-45.

Whyte, J. (2018b). Psychological War in Vietnam: Governmentality at The United States Information Agency. *Geopolitics*, *23*(3), 661-689.

Zehfuss, M. (2012). Culturally sensitive war? The Human Terrain System and the seduction of ethics. *Security Dialogue*, *43*(2), 175-190.

Zehfuss, M. (2013). Staging war as a cultural encounter. In Edkins, J., & Kear, A. (Eds.) *International Politics and Performance: Critical aesthetics and creative practice*. Routledge.

[4] http://www.sfu.ca/publicsquare/community-summit/2019-community-summit.html

Fieldwork for my project will be interspersed throughout the tenure of the fellowship, revolving around attendance at national and international cybersecurity conferences and events. Though conference dates and locations for the 2019-2020 season have yet to be announced, several key events are likely to be held within the UK, such as the Cyber Defense & Network Security Conference (London), the Cyber Threat Intelligence Symposium (London), and the Cybersecurity X Manchester conference (Manchester). I propose to attend as many such events within the UK as possible, limiting fieldwork abroad to the most relevant international conferences such as the Annual Cyberwarfare Symposium (New York), InfoWarCon (Washington, D.C.), the International Cyber Warfare and Security Conference (Turkey), the European Conference on Cyber Warfare and Security (Portugal), and the International Conference on Cyber Warfare and Security (South Africa). When conference dates are announced I will finalize a research itinerary with my co-applicant, not to exceed 30 days abroad per year, allowing me to attend up to ten three-day conferences, six five-day conferences, or any combination thereof.