NISA CONFERENCE 2019

Old wine, new bottles? The transforming discipline of intelligence collection

A warm welcome to The Netherlands!

Dear participant,

We are very happy that you have come to join us at our conference 'Old wine, new bottles? The transforming discipline of intelligence collection'. The Netherlands Intelligence Studies Association (NISA) is glad that so many interesting speakers and participants have come to gather at our international conference of 21 November 2019.

As an association of former intelligence practitioners, academics, and other members with an interest in the intelligence practice, NISA was established in 1991 to further knowledge about intelligence and security related topics. The main aim is to exchange views and to encourage informed debate about intelligence and security services. One of the ways in which NISA does this is by organising international conferences, such as the one today.

Today's topic, in our view, lies at the heart of the intelligence studies: we are discussing the trade as such. Since their institutionalisation, intelligence and security services have developed and trained themselves in unique human and technological collection processes to obtain specific shielded information of interest to them. Particularly after the Cold War, when their legitimate existence was challenged in many Western democracies, it was this unique collection capability that defined their identity; it set them apart from any other branch of government. But now, as the 21st century is progressing, we observe massive changes in the global security architecture and the field of intelligence. Punctuated by 9/11, this century saw the emergence of new threats and new actors, with terrorism becoming the main security concern. This, alongside technological developments and new global governance norms in democracies, has changed the security environment. The Intelligence Community has had to adapt to this new environment, its new roles within national security, and the wider global changes. As a result, its tradecraft, most notably intelligence collection, has undergone significant changes.

This raises many questions. Are intelligence collection disciplines totally different from the 20th century; are sigint and humint qualitatively different activities now than two decades ago? Have their fundamentals changed, has their role in the entire intelligence production process? In our view, the time has come to take stock of where the intelligence community stands in terms of collection. There is a need for a wide and comprehensive overview of the development of intelligence collection – it is not possible to compartmentalise this from broader societal changes, and from changes in different collection disciplines; all the issues are closely intertwined.

We hope to explore what these geopolitical, technological, and societal transformations actually consist of and what their impact on intelligence collection is. In order to do so, we are honoured that a variety of speakers has joined us today. We hoped to bring together men and women from various academic and professional disciplines, various parts of the world, and in various stages of their careers in order to have as many different perspectives on the transforming trade of intelligence collection as possible. In keynote sessions, plenary presentations, and break-out sessions, and in a final panel debate and discussion with all participants, and of course over coffee, lunch, and drinks, we hope to address many aspects of this complex question.

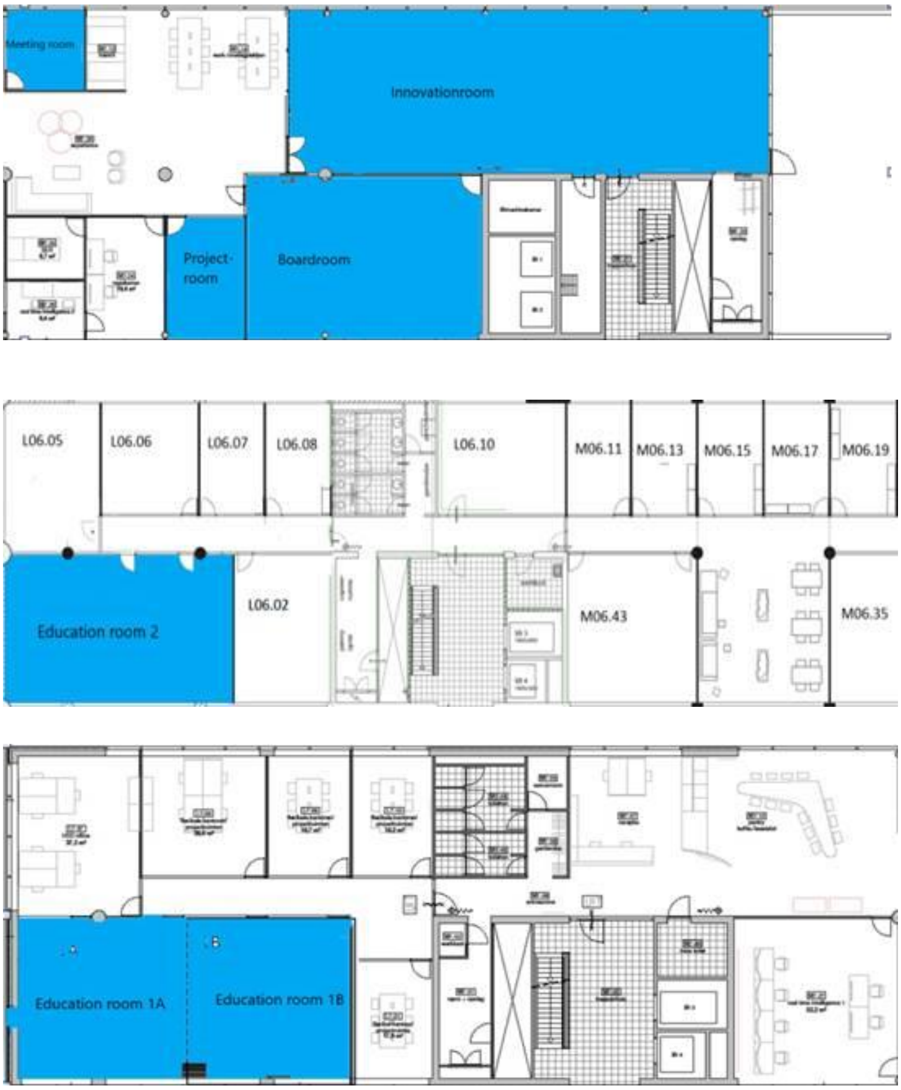
We hope it will be an exciting and fruitful day for all of us. Thanks again for joining us and we hope to keep seeing you on NISA and other events in this field.

Enjoy your stay!

Warm regards,

Constant Hijzen
Chair of NISA

VENUE INFO



Keynote speeches held in Innovation Room.
Break-out sessions held in:
1) Education Room 1A+1B (combined)
2) Education Room 2 (6th floor)
3) Innovation room

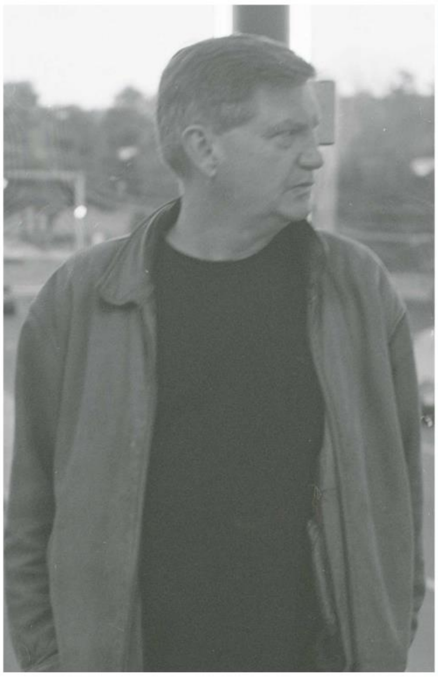
WIFI Code:
Network: Gasten
Password: publ!c!nternet

@NISAssociation
#NISA19

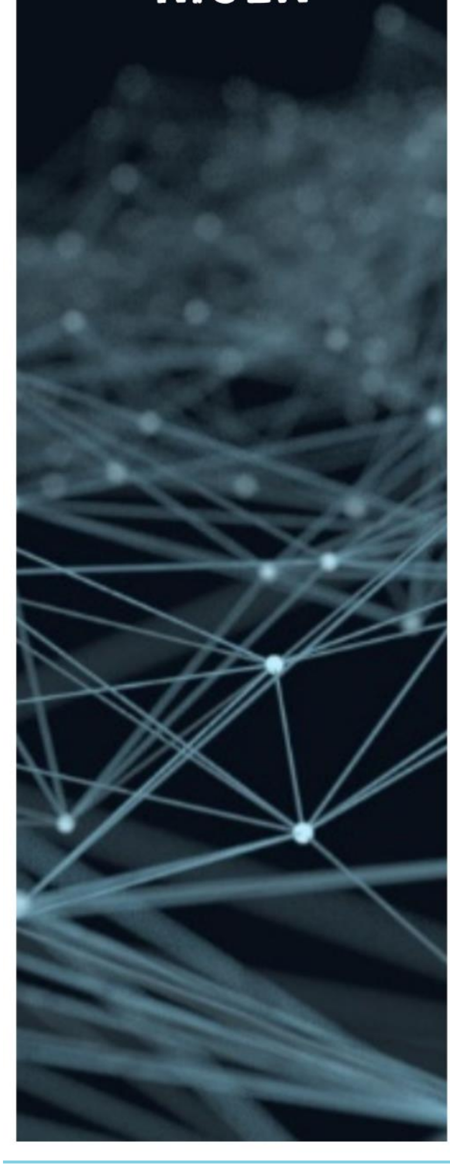
Schedule

8:00 – 8:45	Registration
8:45 – 9:00	Opening words
9:00 – 9:45	Keynote 1: James Risen *Press Freedom in the Age of Technology*
9:45 – 10:30	Plenary session 1: Michael Fredholm *Police Intelligence Collection & National Security Intelligence*
10:30 – 11:00	Break
11:00 – 12:00	Workshop 1 ■ Track 1: Przemysław Gasztold *Sex, Blackmail & HUMINT* ■ Track 2: Elsine van Os *Chinese Intelligence Collection* ■ Track 3: Silviu Paicu *A dangerous method: the use of bulk hacking*
12:00 – 13:00	Lunch
13:00 – 13:45	Keynote 2: Paul Killworth *Intelligence, Technology & Trust in the Cyber Age*
13:45 – 14:30	Plenary session 2: Lonneke van der Velden *OSINT as Public Practice: An Inquiry Into New Methods of Trust Building*
14:30 – 15:00	Break
15:00 – 16:00	Workshop 2 ■ Track 1: Samuel Matsiko *Cyber Arms, Legal Tools & Social Media Surveillance in Uganda* ■ Track 2: AIVD Case ■ Track 3: Christopher Nehring *Cyber, Cyborgs & Social Engineering*
16:00 – 16:45	Keynote 3: Ron Deibert *The Coming Dark Age in Global Cyberspace*
16:45 – 17:45	Panel Discussion with Keynote Speakers, Mr. Schoof & Mr. Reyn
17:45 – 19:00	Closing & drinks

Keynote Speakers



JAMES RISEN



PRESS FREEDOM IN THE AGE OF TECHNOLOGY

James Risen is the senior national security correspondent and columnist for The Intercept, and director of the First Look Press Freedom Defense Fund. He joined First Look and The Intercept in 2017.

Before that, he worked for The New York Times for 20 years, covering the Central Intelligence Agency and national security as an investigative reporter based in Washington. He was the winner of the 2006 Pulitzer Prize for national reporting. He was also a member of the New York Times reporting team that won the 2002 Pulitzer Prize for explanatory reporting. He was also the winner of the 2006 Goldsmith Prize for investigative reporting. He previously worked at the Los Angeles Times.

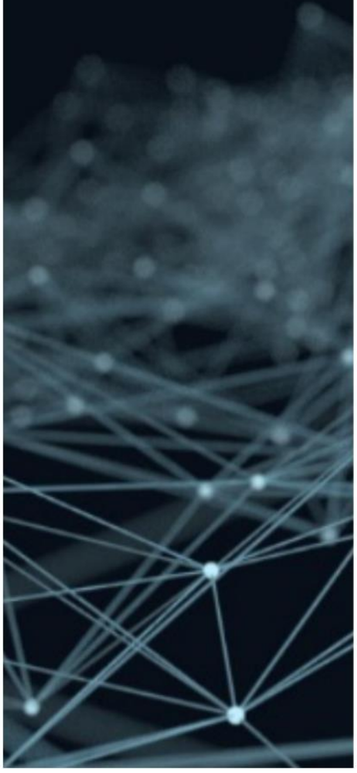
He is the author of four other books. Risen was elected to the American Academy of Arts and Sciences in 2007. In 2012, he received the John Aubuchon Press Freedom Award, from the National Press Club.

In 2014, he received the Stephen Hamblett First Amendment Award, from the New England First Amendment Coalition. He received the Elijah P. Lovejoy Award, from Colby College, in 2014, which also awarded him an Honorary Doctor of Laws Degree. In 2014, he received the Newspaper Guild's Herbert Block Freedom Award.

In 2015, he received the Ridenhour Courage Prize. He received the Constitutional Champion Award, from The Constitution Project, in 2015. In 2015, he received the Hugh M. Hefner First Amendment Award, from The Playboy Foundation. He was inducted into the Medill School of Journalism Hall of Achievement in 2015.

In 2017, he received an honorable mention from the Dart Awards from the Dart Center for Journalism and Trauma at the Columbia School of Journalism for a series on the long-term psychological effects on detainees of the U.S. torture program. Risen waged a campaign for press freedom against the government that lasted nearly a decade.

Paul Killworth



Intelligence, technology and trust in the cyber age

Intelligence, technology and trust in the cyber age. The intelligence that keeps our societies secure depends on advanced technology, more so than ever before. In recent years, however, technology has become part of the global geopolitical race, bound up with issues of national security, prosperity and ethics. This talk will present a practitioner's perspective on the changing world of intelligence and technology, examining the relationship between trust and power in the cyber age."

Dr Paul Killworth is the Deputy Director Strategic Policy in GCHQ. He joined the organisation in 1998, following an academic career as a Social Anthropologist, and has since worked in varied operational and policy areas. He headed GCHQ's Cyber strategy for several years and was closely involved in the Investigatory Powers Act (2016).
He has also worked for the Ministry of Defence in Iraq and the Balkans, for the Foreign and Commonwealth Office as a Political Counsellor in British Embassy Kabul and was a member of the 2015 Strategic Defence and Security Review team in the Cabinet Office.
Paul is married, with three children; in his limited spare time, he studies medieval history, writes and talks on emerging technology, privacy and security issues, and occasionally still codes software.

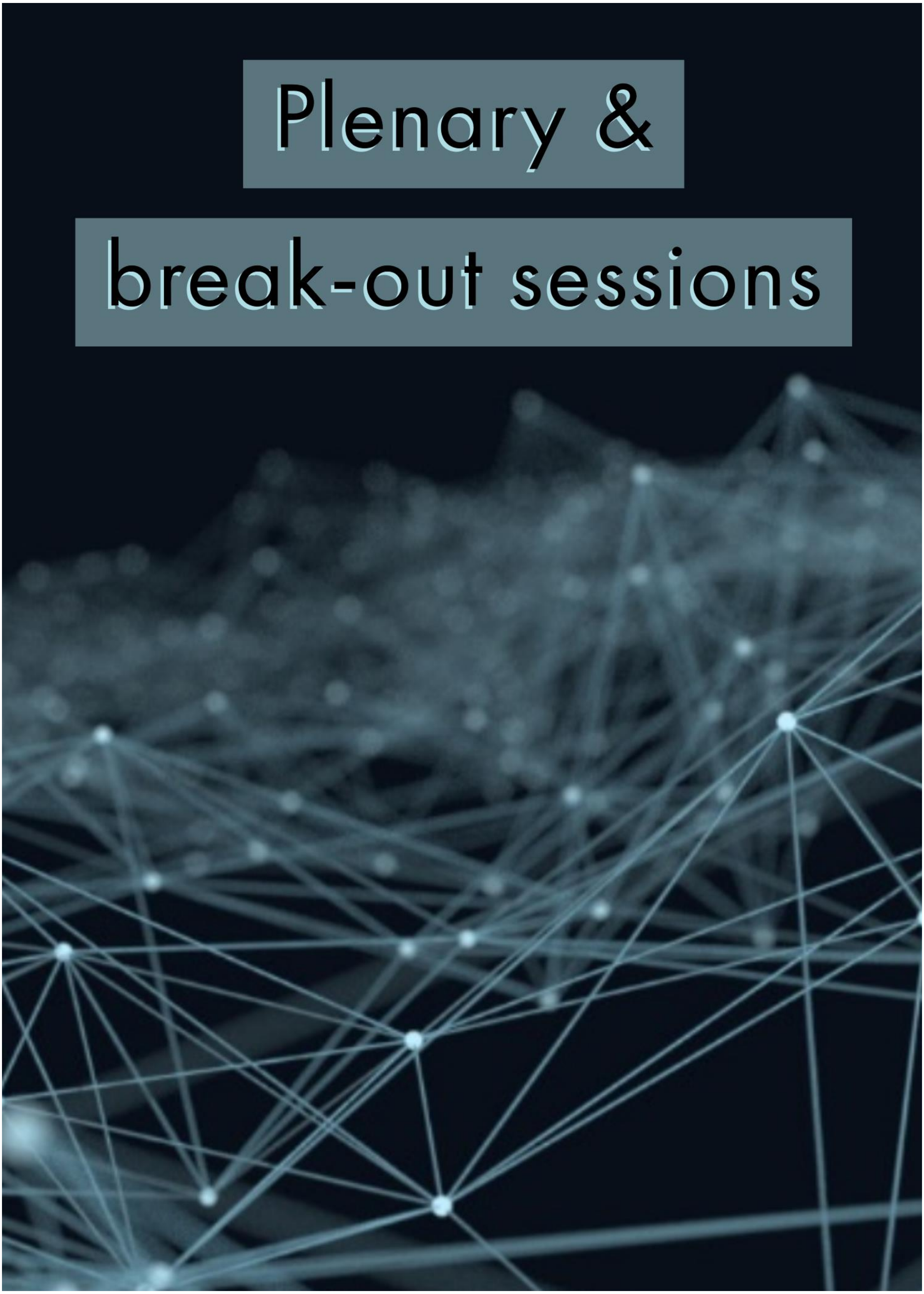
RONALD DEIBERT

THE COMING DARK AGE IN GLOBAL CYBERSPACE

Political struggles in and through the global Internet and related technologies are entering into a particularly dangerous phase for openness, security, and human rights. A growing number of governments and private companies have turned to "offensive" operations, with means ranging from sophisticated and expensive to home-grown and cheap. A large and largely unregulated market for commercial surveillance technology is finding willing clientele among the world's least accountable regimes. Powerful spyware tools are used to infiltrate civil society networks, targeting the devices of journalists, human rights defenders, minority movements, and political opposition, often with lethal consequences. Meanwhile, numerous disinformation and harassment campaigns are feeding intolerance and even violence, largely without mitigation. Drawing from the last decade of research of the University of Toronto's Citizen Lab, I will provide an overview of these disturbing trends and discuss some pathways to repairing and restoring the Internet as a sphere that supports, rather than diminishes, human rights.

Ronald J. Deibert is Professor of Political Science and Director of the Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto. The Citizen Lab undertakes interdisciplinary research at the intersection of global security, ICTs, and human rights. The research outputs of the Citizen Lab are routinely covered in global media, including over two dozen reports receiving front page coverage in the New York Times, Washington Post, and other media over the last decade. Deibert is the author of Black Code: Surveillance, Privacy, and the Dark Side of the Internet (Random House: 2013), as well as numerous books, chapters, articles, and reports on Internet censorship, surveillance, and cyber security. In 2013, he was appointed to the Order of Ontario and awarded the Queen Elizabeth II Diamond Jubilee medal, for being "among the first to recognize and take measures to mitigate growing threats to communications rights, openness and security worldwide."

Plenary & break-out sessions



Plenary Sessions

Michael Fredholm

Police Intelligence Collection and National Security Intelligence

Until 1945, police intelligence remained a key source of national intelligence. Of particular importance for counterespionage and counterterrorism, police networks also provided strategic intelligence on countries with which police cooperation took place an, in times of war, facilitated operations on enemy territory. From 1929, for instance, the Cairo Police coordinated a global intelligence network ranging from Europe to China and the United States which although primarily dealing with the international narcotics trade also combated political unrest. From 1934, U.S. law enforcement combated first German, then Soviet intelligence activities, and from 1940 in Central and South America as well. From 1942, Swedish police liaised with and supported resistance movements in Nazi-occupied Europe at the same time that they also collected intelligence through liaison with the German Gestapo. By dealing with both sides in a conflict, police intelligence not only acquired comprehensive data but also enabled second-track negotiations. However, with the Cold War emergence of more formalized and compartmentalized national intelligence services, police intelligence collection was gradually disregarded. This mindset continued until the 9/11 terrorist attacks which again brought national intelligence out of the diplomatic reception rooms and onto the streets of dangerous neighborhoods. Voices were again heard arguing for the use of international police networks for national intelligence collection. I will describe the different police collection disciplines, address how police intelligence collection has evolved under conditions of increasing oversight and privacy concerns, and argue for the importance of including police intelligence collection in a variety of national intelligence tasks.

Professor Michael Fredholm is an historian and former military analyst who has published extensively on the history, defense strategies, security policies, intelligence services, issues related to terrorism, and energy sector developments of Eurasia. He currently is the Head of R&D at IRI, an independent research institute. IRI emerged out of the work carried out at the Stockholm International Program for Central Asian Studies (SIPCAS), where Michael Fredholm made a special study of Central Asian geopolitics, Islamic extremism, and counterterrorism. He has worked as an independent academic advisor to governmental, inter-governmental, and non-governmental bodies for more than 2 decades. Michael Fredholm also led the team which developed the lone actor terrorism counter-strategy and training program for the Swedish National Bureau of Investigation and Swedish Police Authority, which was implemented in 2014-2015. He participates in the work of the editorial committee of the History Project of the Swedish signals intelligence service, the FRA. He also regularly conducts research at the Swedish Military Archives.

Lonneke van der Velden

OSINT as public practice: An inquiry into new methods of trust building

In the past few years we have seen collectives and action groups emerging that engage with online open source intelligence gathering. BellingCat and Syrian Archive are examples of collectives that make use of the enormous pool of social media data, satellite images, and circulating leaks and have developed their own tools and methods for data analysis. Syrian Archive, for instance, uses OSINT for documenting human rights violations in Syria by curating images circulating on social media. In this presentation, I suggest exploring the emerging phenomenon of OSINT as 'public practice', that is, OSINT that takes place in close conversation with the public domain. Its practitioners articulate public aims, publish their findings widely, and try to educate the public by sharing skills. For some this includes the use of tools that are licensed under a free license to allow public inspection. This presentation is about OSINT in which civil society is not just a 'partner', but rather becomes the main driver.
The paper treats public OSINT as a specific 'epistemic culture' with its own specific protocols and style of digital truth finding. By doing a closer reading of 'public' OSINT projects (which principally engage with the public domain) I explore how they organise knowledge production, by looking at which values influence the choice of methods and tools, and the extent to which standards are emerging that bind these OSINT practitioners as a 'community of practice'. In other words, the paper takes a look at the social environment of a very specific and alternative intelligence community. Given the lack of institutional accreditation, the question becomes, for both OSINT practitioners and for scholars, how trust is built and how public trust is connected to open source methods and ideals.

Lonneke van der Velden is a postdoctoral researcher at the ERC funded research project DATACTIVE at the University of Amsterdam (UvA). DATACTIVE explores the politics of big data broadly defined. The project takes a critical look at datafication and investigates the responses by social movements and civil society. Lonneke's work within the project focuses on Open Source Intelligence practices by civil society actors. She also teaches at the New Media and Digital Culture program (UvA). Next to her work, she is part of the editorial board of Krisis, journal for contemporary philosophy in the Netherlands, and member of the Board of Directors of the Dutch digital rights organisation Bits of Freedom.

Break-out Sessions

Sex, Blackmail and HUMINT: New Evidence on the Effectiveness of the Polish Intelligence Honey Trapping Operations During the Cold War

Przemysław Gasztold

11:00-12:00

A share of the recently released documents from the Polish "restricted collection" – the Cold War files – consists of the operational files from the Polish civilian counterintelligence (Departament II MSW), which was responsible for vetting and recruiting spies among the diplomats and foreigners who lived in or travelled to Poland. The analysis of several dozen cases revealed the frequent use of honey traps, as well as other forms of blackmail, as plots to force people to become the sources of confidential information. On the other hand, however, the declassified documents indicate a surprisingly poor effectiveness of such dirty tricks and pose serious questions about the quality of HUMINT gained by coercion.

In my paper, I will describe several blackmail operations conducted by the Polish counterintelligence services, which were aimed at recruiting diplomats and foreign citizens. I will present how honey traps were prepared, set up, and executed. Then, I will reassess their long-term efficiency. I will also evaluate the effectiveness of the sources who initially agreed to work as spies, and will show whether such a cooperation withstood the test of time. Finally, the comparison of failed and successful "sexspionage" operations will be put into the context of a broader framework of Human Intelligence. This will allow me to address the question of psychological and moral dilemmas resulting from the use of coercion in modern espionage.

Przemysław Gasztold (Ph.D.) is a research fellow at the Historic Research Office of the Institute of National Remembrance in Warsaw and Assistant Professor at War Studies University in Warsaw, Department of Security Threats and Terrorism. He received his Ph.D. from Warsaw University, Faculty of Journalism and Political Science, in 2016. He is currently conducting research on Polish Intelligence, on relations between Poland, the Middle East, and Africa, and on the ties between the Soviet bloc and international terrorism during the Cold War. Alumnus of US State Department Study of US Institutes on National Security Policymaking (University of Delaware, 2019). His recent book Towarzysze z betonu. Dogmatyzm w PZPR 1980-1990 ("Comrades of Concrete. Dogmatism within the PUWP 1980-1990) was published in 2019. Co-editor (with A. Hanni and T. Riegler) of Terrorism in the Cold War: State Involvement and Covert Operations. Volume 1: Eastern Europe and the Soviet Sphere of Influence; Volume 2: The West, the Middle East and Latin America, IB Tauris/Bloomsbury Publishing [forthcoming]. Member of the "Need to know" conference's organizing committee. He may be contacted at przemyslaw.gasztold@ipn.gov.pl or p.gasztold@akademia.mil.pl

The comprehensive strategy behind the rise of China: Chinese intelligence collection

Elsine van Os

11:00-12:00

According to the US, Canada, Australia and the United Kingdom, China has been at number 1 for years in terms of economic espionage. Around 70% of all Chinese espionage is aimed at the high-tech industry. The ambition of the political leaders in Beijing is to become the world's technology leader by 2025. When we talk about Chinese espionage, we primarily think of hacking. However, the range of Chinese espionage methods with the aim of stealing intellectual property from companies is much broader. The way in which China tries to become the superpower of the world is not through traditional methods such as weapons, but through technological advances. In addition, economic espionage seems to revolve around money and the economy, but in reality, it is about influence and dependence. It is very difficult for companies, the government and society to recognize this problem. Are companies capable of recognizing espionage? Do companies look closely at the partnerships they have entered into, who they have in-house? Do they know what to look out for? And, more importantly: do they want to know?

Elsine van Os is a clinical psychologist and intelligence and security specialist who has integrated her skills in Insider Risk Programme training and consultancy to both the public and private sectors. In that domain she works on the nexus between (cyber) security and social sciences. She is the founder and CEO of Signpost Six, Insider Risk Management consultancy firm and Signpost Film Productions which released a documentary about Edward Snowden last year.

A dangerous method: the use of bulk hacking in large-scale operations by the security and intelligence services and its transformative impact on the process of intelligence collection

Silviu C. Paicu

11:00-12:00

Europe has witnessed in the last several years a proliferation of national intelligence laws with a bulk collection dimension. This expansion of governmental surveillance powers at European level is also reflected by the stream of landmark judgments issued by the European Court of Human Rights which clearly established that bulk interception of foreign communication is a valuable resource in the fight against terrorism. However, the fading efficiency of bulk interception due to enhanced encryption has made bulk equipment interference or hacking more necessary than ever for retrieving valuable intelligence. This piece of research explores the challenges raised by the growing utilisation of bulk hacking as a collection method and its transformative influence on the classic conceptual model of intelligence collection. Taking the UK as a case study, it examines how bulk equipment interference is deployed and regulated in a country with one of the most resourceful oversight systems in the world. With bulk hacking already an operational reality in the international arena, the challenge for the democratic governance is how to increase the legitimacy and effectiveness of this controversial practice.

I am currently a PhD Candidate in Intelligence and National Security at "Mihai Viteazul" National Intelligence Academy in Romania and at University of Malta and also a Marie Curie Early Stage Researcher in Security Science. My doctoral research which started in October 2017 investigates the existing societal debates on bulk collection powers in the UK and the Netherlands with a focus on the transformation of intelligence oversight. I hold an MA in Politics and Security with a post-Soviet regional focus from University College London (UCL), and a BA in Politics from Queen Mary, University of London. Also, I have been awarded several academic scholarships and grants and worked for a short period in the private intelligence sector. My other research interests include civil-military relations, security sector governance and critical approaches to security.

Cyber Arms, Legal Tools and Social Media Surveillance in Uganda

Samuel Matsiko

15:00-16:00

On 18th February 2016 as Ugandans went to the polls for a general election the government of Uganda cut off access to social media platforms including Facebook, Whatsapp, and Twitter. That day Ugandans got baptized into the world of virtual private networks. You could tweet from a server in the Netherlands and vote in Uganda at the same time. According to Trust. Zone, a VPN provider, there were more than half a million VPN downloads from Uganda on election day. Uganda's Internet usage has continued to grow in recent years with over 14 million people connected to the Internet out of a population of over 41 million people. The majority of the users are connecting via mobile-enabled devices. The growth in electronic protests, hacktivism, and internet usage has in equal measure attracted interest from the state and security agencies to control and monitor users these activities. Uganda's intelligence community has invested in several surveillance tools and cyber arms to curtail dissent. These cyber arms include but not limited to intrusion malware, social media monitoring software, and facial recognition surveillance. Uganda has also put in place over ten pieces of legislation or legal tools to legitimize this form of surveillance conducted by the intelligence community. The most notable legal tool is the Regulation of Interception of Communications Act. This paper aims to explore the recent trends in global security architecture and the emerging digital environment in Uganda with a focus on the intelligence community and social media surveillance. The paper will critically look at the modes of intelligence collection and the legal environment enabling mass surveillance in Uganda with a focus on social media.

Samuel Matsiko is a lawyer by training and a senior research fellow at the Amsterdam Center for War Reparations. He is an early career investigator with the global atrocities constellations research group based at the University of Copenhagen as a recipient of the European Union 2020 Horizon Grant. Samuel Matsiko has taught international law at the Uganda Christian University and served as the Vice President of the International Law Association Uganda.
In 2016, the Dutch Ministry of Foreign Affairs and the Netherlands Society for International awarded Samuel Matsiko the Young African Scholars for International Law Award. In 2017, he represented Uganda at the United Nations International Law Commission in Geneva and served on the working group on Universal Jurisdiction. Prior to academia, Samuel Matsiko worked with International Justice Mission and served as a reporter for the Oxford International Law in Domestic Courts (ILDC) reports a project of the Amsterdam Center for International Law. Samuel holds an LLM from Humboldt University.

Cyber, Cyborgs and Social Engineering – A Cultural Studies' approach to HUMINT in the Cyber Age

Christopher Nehring

15:00-16:00

In the years after Edward Snowden intelligence research focused largely on technological means of information gathering. However, the Skripal-poisoning or the murder of Jamal Khashoggi indicated a "renaissance" of HUMINT, both in intelligence practice as well as intelligence research. Yet, while old fashioned killing operations have hardly changed, other aspects, definitions, applications and conceptualizations of HUMINT are heavily influenced by digitalization and cyber. Concepts and terms such as "Cyber-HUMINT" or "social engineering" reflect this development. The human and the digital, HUMINT and CYBINT seem to be in a process of "fusion". Some scholars see "cyber" as an intelligence revolution, while others argue that it is an intelligence evolution rather than a revolution and that classical HUMINT continues to be of utmost importance.
This paper examines HUMINT in the cyber era from three sides: First, I will introduce existing theories and concepts (e.g. Cyber HUMINT, Cyber-induced HUMINT / HUMINT-induced Cyber, Social engineering, Cyborg); second, I will try to identify aspects of HUMINT that are influenced and altered by the advent of digital technology; third and last, I will use the Cultural Studies' theory of Posthumanism to offer an explanation and conceptualization of HUMINT in the cyber era. The value of Cultural Studies to intelligence research has recently been demonstrated and posthumanistic approaches to the ongoing fusion of humanity and technology, the deconstruction of Humanism and making sense of the crisis of human identity in the digital age have a lot to offer for understanding the unease about HUMINT in the cyber age.

Dr. Christopher Nehring is Academic Director German Spy Museum, Berlin, Germany. He has a PhD in Intelligence and Eastern European History from the University of Heidelberg, Germany.

Intelligence & oversight: a (fictional) case study with the AIVD

15:00-16:00

The AIVD will provide an interactive walkthrough of the way of working under the Intelligence & Security Services Act of 2017, using a fictional but realistic case study. Through the reconstruction of an intelligence operation, the legal and moral responsibilities that the AIVD and the oversight body carry will be explored.

Sponsors

NISA would like to thank the following sponsors for helping make this conference possible.

HSD
The Hague Security Delta

VREDE EN RECHT
The Hague

dcypher

Sign post Six
PSYCHOLOGY FOR INTELLIGENCE AND SECURITY

POLITIE
Politieacademie

Ministerie van Defensie

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Conference Team

Constant Hijzen
Elsine van Os
Matthijs Koot
Clotilde Sebag

NETHERLANDS INTELLIGENCE STUDIES ASSOCIATION
NISA

A warm thank you to
Tom Schoen & Jonas Carinhas for their assistance.