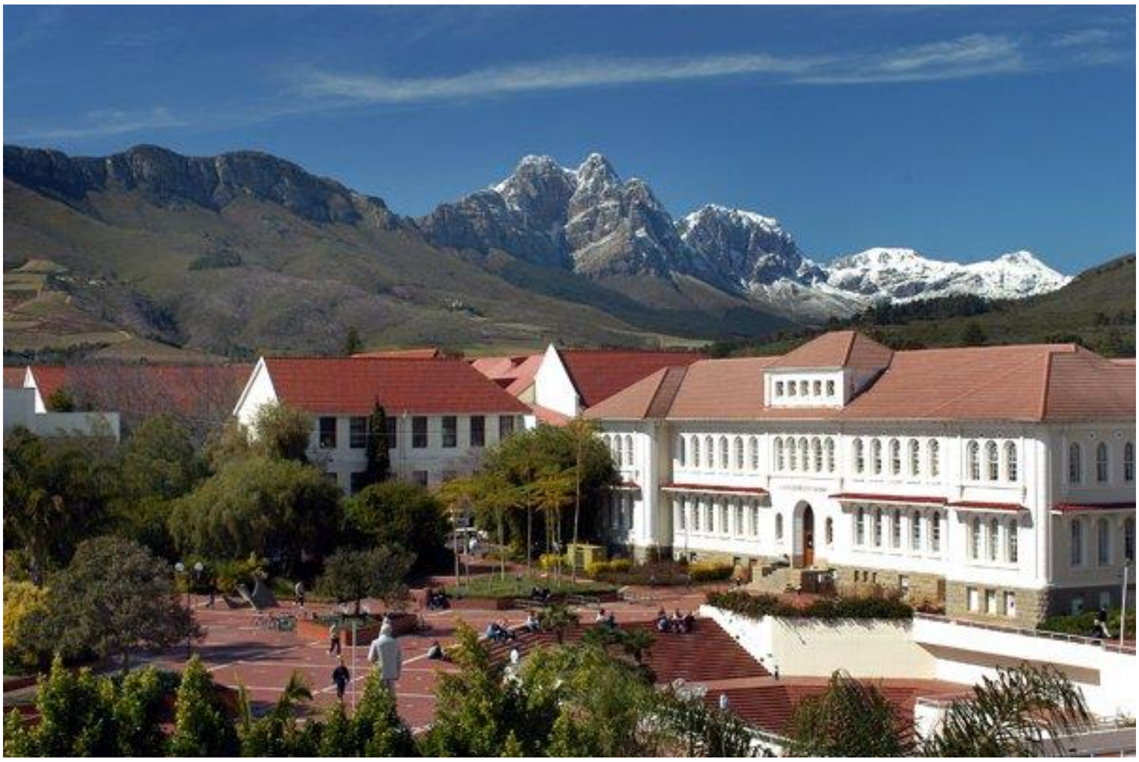
Darya Bazarkina, Jaivin Van Lingen, Olga Polunina

Russian Researchers on Strategic Communication in South Africa: Focusing on the Malicious Use of Artificial Intelligence

DSc. Prof. Evgeny Pashentsev, leading researcher at the Institute of Contemporary International Studies of the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, director of the International Centre for Social and Political Studies and Consulting (ICSPSC), coordinator of the GlobalStratCom international strategic studies associations project, the Russian – Latin American Strategic Studies Association (RLASSA), European-Russian Communication Management Network (EU-RU-CM Network) and Dr. Olga Polunina, a researcher at the ICSPSC took part in several academic events in South Africa in February 28 – March 11 2019 in South Africa. Konstantin Pantserev, a coordinator of African Strategic Studies at the ICSPSC and professor at Saint-Petersburg State University joined them in Stellenbosch. The trip was organized and supported by ICSPSC with a kind assistance of their partners in South Africa. Prof. Darya Bazarkina and Doctoral student Jaivin Van Lingen interviewed Prof. Evgeny Pashentsev and Dr. Olga Polunina and presented with her participation the following summary of the trip and the post-trip analysis of Russian specialists.

Stellenbosch

On February 28 – March 1 Russian researchers contributed to the mini-track “Psychological Warfare, New Technologies and Political Instability in Contemporary World” at the 14th International Conference on Cyber Warfare and Security - ICCWS 2019 which is being hosted by Stellenbosch University and the CSIR at Stellenbosch University, South Africa.



Stellenbosch University

ICCWS conferences is a good opportunity for academics, military personnel, practitioners and consultants from around the world who are involved in the study, management, development and implementation of systems and concepts to combat information warfare or to improve information systems security to come together and exchange ideas. There are several strong strands of research developing in the cyber warfare and cyber security area including the understanding of threats and risks to information systems, the development of a strong security culture, as well as incident detection and post incident investigation. New threats brought about by social networking and cloud computing are gaining interest from the research community and the conference is tackling these issues. The conference in Stellenbosch was continuing to establish itself as a key event for individuals working in the field from around the world.

The hosting organization – *Stellenbosch University* is jointly the oldest university in South Africa alongside the University of Cape Town (UCT) which received full university status on the same day in 1918. Stellenbosch University is the second-highest ranked African University according to the 2017-2018 QS World University Rankings. ICCWS 2019 hosted by SU in conjunction with the Council for Scientific and Industrial Research (CSIR) was presented by the Security Institute for Governance and Leadership in Africa (Sigla), attached to SU's Faculty of Military Science.

At the plenary session at ICCWS 2019, 28 February 2019

Conference and Programme Chairs: Noëlle van der Waag-Cowling is a military science professional with 25 years of experience in the Department of Defence, South Africa and 20 years of experience in South African Higher Education at Stellenbosch University. She is the co-ordinator of the Cyber Project at the Security Institute for Governance and Leadership in Africa; Louise Leenen is an Associate Professor in Computer Science at the University of the Western Cape in South Africa. She worked as a Principal Researcher focusing on defence related research at the Council for Scientific and Industrial Research in South Africa until the end of 2018. Her areas of specialisation are Artificial Intelligence applications in Cyber Defence and mathematical modeling. She is the Chair of the International Federation for Information Processing's Working.

The conference was opened by the Dean of Military Science and Director of SIGLA, Prof Sam Tshehla with speakers hailing from Africa, Europe, Asia and North America. From a South African perspective, one of the most anticipated keynotes was delivered by Brig Gen Piet Pieterse (SAPS) on Cybercrime as part of a transnational organised crime threat.

Brig Gen Piet Pieterse (SAPS)

The mini-track “Psychological Warfare, New Technologies and Political Instability in Contemporary World” which was initiated and chaired by Prof. Pashentsev attracted a lot of attention of the conference participants. The 21st century has seen a plethora of armed conflicts and revolutions where the elements and tools of Psychological Warfare (PW) have been used to affect the political stability of countries and regions. Information, knowledge and their use has become an integral part in political and armed conflict and psychological warfare is used in parallel to traditional physical combat. This is due in no small part to the fact that the outcomes of war are determined by political rather than military factors. Under such circumstances it is possible to win battles militarily, but ultimately lose the war politically. The ways that these types of conflict are initiated and waged are becoming increasingly sophisticated. One can expect a system usage of a wide variety of new technologies on tactical, operational and strategic levels of psychological warfare.

Topics of the mini-track were aimed to attract attention to the following themes:

- the role and practice of psychological warfare in the modern geopolitical confrontation, civil and military conflicts and counter-terrorist activity;
- new opportunities given to psychological warfare by the combination of Big Data analysis, the results of neuroscience research and nudge technologies. Prognostic weapons;
- artificial intelligence and psychological warfare;
- psychotronic warfare and psychotropic warfare;
- molecular communication in the warfare;
- genetic engineering, cyborgization and psychological warfare;
- psychological effects of biological warfare;
- psychological warfare elements in hybrid warfare, unconventional warfare, counter-unconventional warfare;
- psychological warfare through Internet and social networks;
- strategic deception and new technologies;
- theoretical backgrounds of psychological warfare through new technologies.

Some of these topics found themselves reflected in different papers presented at the mini-track. Among them: *Destabilization of Unstable Dynamic Social Equilibriums through High-Tech Strategic Psychological Warfare* by Evgeny **Pashentsev**, Diplomatic Academy at the Ministry of Foreign Affairs of Russia, Moscow; *Exploring Interactive Narrative and Ideology in War Games by* Anna-Marie **Jansen van Vuuren**, University of Johannesburg and Tristan **Jacobs**, AFDA (School for the Creative Economy), South Africa; *Artificial Intelligence: Playing the Imitation Game* by Jantje **Silomon** Jantje and Monica **Kaminska**, University of Oxford, UK; *Countering Terrorist Propaganda in Asia: Towards a Better Communications Strategy in Cyberspace* by Konstantin **Pantserev** and Konstantin **Golubev**, Saint-Petersburg State University, Russia; *Ethics of Trust in Man-Machine AI Interactions* by Mary **Manjikian**, Regent University, Chesapeake, USA.

Some papers and posters outside the mini-track were devoted at ICCWS 2019 to the topic of psychological warfare: *Smart Algorithms and Psychological Warfare* by Olga **Polunina**, Russian State Social University, Moscow, Russia; *Advanced Technologies Combating Terrorism in the EU: the Psychological Warfare Aspect* by **Darya Bazarkina**, Russian Academy of National Economy and Public Administration under the President of RF. Moscow, Russia; *Fake Narratives, Dominant Discourses: The Role and Influence of Algorithms on the Online South African Land Reform Debate* by **Anna-Marie Jansen van Vuuren,** Department of Journalism, Film and Television, University of Johannesburg, South Africa and **Turgay Celik**, School of Computer Science and Applied Mathematics, Wits University, Johannesburg, South Africa; *Social Media as a Declaration of War?* by **Trishana Ramluckan**, University of KwaZulu-Natal, Westville, South Africa; The Terrorist/Jihadi use of 3D-Printing Technologies: Operational Realities, Technical Capabilities, Intentions and the Risk of Psychological Operations by **Ferdinand Haberl**, Department of Oriental Studies, University of Vienna, Austria and **Florian Huemer**, Institute of Computer Engineering (ECS Group), TU Wien, Austria; Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception by **Martti Kari,** University of Jyväskylä, Finland.

Prof. Evgeny Pashentsev in his paper *Destabilization of Unstable Dynamic Social Equilibriums through High-Tech Strategic Psychological Warfare* analysed the new dimensions for psychological warfare. The extracts from this paper we give below.

Evgeny Pashentsev's presentation at the mini-track "Psychological Warfare, New Technologies and Political Instability in Contemporary World". March 1st, 2019.

At the mini-track “Psychological Warfare, New Technologies and Political Instability in Contemporary World”. March 1st, 2019.

Sophisticated technologies allow to solve many problems, although, due to the imperfection of social relations and human nature itself, these technologies are very often used against humans. Wide opportunities for that are provided by Strategic Psychological Warfare (SPW), which aims at the development of a particular institution, country, or the international system as a whole, in a way that has a desirable direction for the leading actor. SPW uses various channels and means of targeted, systemic, long-term impact on the development of social systems.

The role of advanced technologies in SPW is difficult to underestimate. Many phenomena and techniques fit into the fabric of SPW. The mechanism of using radio and television for such purposes is well known and the Internet has been well mastered for this purpose, but we have a much worse notion of the use of advanced technologies, such as Big Data, AI, etc. within the framework of SPW. It is equally important to know what promising technologies can enhance psychological warfare abilities in the foreseeable future. Today insufficient attention is being paid to the comprehensive analysis of the issues of the Unstable Dynamic Social Equilibriums (UDSE), which are especially vulnerable in the context of random and targeted negative impacts in the field of High-Tech SPW. The hypothesis of Prof. Pashentsev study is that sophisticated technologies raise the SPW to a qualitatively new level, which requires an adequate assessment and reaction, not only from the military institutions, but from society as a whole.

AI radically increases the ability of the human mind to influence the target audiences (through deep fakes, fake people and other new forms of efficient tools of perception management). AI also increasingly makes it possible to foresee the specific parameters of individual events and allows for identification of the effectiveness of influence operations much faster and more effectively. Thus, AI takes one of the leading places among other means and methods of offensive HTSP. It, however, creates new adequate capabilities of defensive HTSP, which is typical for the dynamic unstable balance of all offensive and defensive weapons.

Today Russia, China, USA, the EU, and their HT partners, in spite of their contradictions, have to pay more attention to the discussion at the expert level, at first not only on the dangerous consequences of the nuclear arms race, the technical aspects of cybersecurity, but also of the dangerous threats of the modern HTSPW. It will be a win-to-win game because HTSPW increases the risks of WW3. Through the use of new technologies, it is more and more easy, under unstable dynamic social equilibriums, to provoke, in a latent way, a dangerous error, wrong decision-making process of top militaries, politicians by the extremist “third party”, which aims global destabilization by all means, in spite of the tragic global consequences (for example, by terrorist organizations, etc.).

The current level of technology, and not least, AI, seriously affects the capabilities of SPW. The speed, scale and depth of impact are increasing (up to the creation of a life-long artificial reality for individuals and target groups). Without the development of a person as a harmoniously developed individual, it is impossible to talk about an effective system of security of society and the person from information and psychological threats. The potential of civil society, free associations of citizens on the Internet to protect digital freedom and citizen empowerment (and not the mass consumer, as it, alas, now often happens) should be used. The author is not against the protection of consumers, and citizens, they are entirely for. But protection of consumers without their own civic awareness and social activism initially has little chance for success. The mass consumer easily becomes a victim of bothegoistic corporate groups and terrorist organizations, geopolitical games etc., although it is impossible to identify them in the majority of cases. The mass consumer becomes a victim due to easily calculable and obvious reactions. The development of a fully developed and active individual living in harmony with social interests is a reliable guarantee of the development and strengthening of democracy and the creation, in particular, of a reliable barrier to the spread of destructive influence campaigns, whether they originate from state or non-state actors.

We can note the triumph of professionalism at the conference in Stellenbosch, the spirit of mutual respect in scientific discussions, the lack of a pronounced anti-Russian attitudes, despite the large number of experts from NATO countries. Apparently, those who have a substantive understanding of the problems of cybersecurity are well aware of how many vulnerabilities all sides of the global confrontation in the international arena have and how dangerous the consequences of further escalation of the situation are. Alas, not all politicians can have such understanding or they carefully hide this understanding from the public in favor of the interests of the military-industrial complex. The problems are growing at the global, regional and local levels. The on-going crisis on the world arena, of course, could not but affect the mood of the conference participants and the contents of some discussions. However, the excellent organization of the conference itself and friendly communication on the conference sidelines determined its success. Academic Conferences and Publishing have been supporting the Academic Community for over 20 years and manage a range of Conferences Worldwide and success of ICCWS 2019 is also their success.

Dr. Olga Polunina at the conference break

The conference at Stellenbosch proved the permanent and rising role of Russian researchers at the international academic forums where are under debate the hot issues of international psychological security and psychological warfare.

Cape Town

In Cape Town Prof. Evgeny Pashentsev and Dr. Olga Polunina visited the *University of Cape Town (UCT)*. The university was founded in 1829 as the South Africa making UCT the oldest higher education institute in South Africa. UCT is the highest-ranked African university in the QS World University Rankings.

University of Cape Town (UCT)

Professor Evgeny Pashentsev presented his talk at the seminar entitled**,** "Artificial Intelligence and the challenges to international psychological security on the internet." The research seminar took place March 4 at the Department of Political Studies at UCT with the kind support of the head of the department Assoc. Prof. Thiven Reddy and Dr Elias Phaahla, the lecturer of the department. The Department of Political Studies is home to internationally recognised scholars in comparative politics, international relations, political theory, political behaviour, intellectual history, public policy, and public administration. The members of the Department have made contributions to a range of government activities especially in the areas of defense, development, education, local government, mediation, policing and voting.

In his talk prof. Pashentsev focused on the possible malicious use of AI (MUAI) threats that can cause serious destabilizing effects on the social and political development of different countries and the system of international relations, including the sphere of IPS.

Big Data, Predictive (Prognostic) Weapons: To the New Horizons in Management of Political Conflicts

- Early Model Based Event Recognition using Surrogates (EMBERS).The case study of Venezuela
- Ground truth data (called the gold standard report {GSR})

Source: Big Data N. December, 2014. P. 193.

Evgeny Pashentsev's presentation at the University of Cape Town (UCT)

The following MUAI classification according to the degree of implementability is possible:

- current MUAI practices;
- existing MUAI capabilities that have not been used in practice yet (this probability is associated with a wide range of new rapidly developing AI capabilities — not all of them are immediately included in the range of implemented MUAI capabilities);
- future MUAI capabilities based on current developments and future research (assessments should be given for the short, medium and long term);
- unidentified risks, also known as "the unknown in the unknown." Not all AI developments can be accurately assessed. Readiness to meet unexpected hidden risks is crucial.

The speaker presented some examples of MUAI through Internet and not only, among them:

- ***The growth of integrated, all-encompassing systems with active or leading AI use*** increases the risk of malicious takeover of such systems. Numerous infrastructure facilities, for example, robotic self-learning transport systems with AI-based centralized management, can be convenient targets for high-tech terrorist attacks.
- ***The creation of 'deepfakes'***. 'Deepfake' (a portmanteau of "deep learning" and "fake") is an AI-based human image/voice synthesis technique. Many celebrities, including Scarlett Johansson, Maisie Williams, Taylor Swift and Mila Kunis, have fallen victim to deepfake pornography. Deepfakes hobbyists have begun using this technology to create digitally-altered videos of world leaders, including U.S. President Donald Trump, Russian President Vladimir Putin, former U.S. president Barack Obama and former presidential candidate Hillary Clinton. Experts warn that the videos could be realistic enough to manipulate future elections and global politics as early as 2020. However, it could take years before researchers invent a system that can reliably detect deepfakes, which makes them a potentially dangerous lever for influencing the behavior of individual persons and large target groups. Deepfakes can be used in psychological warfare to provoke financial panic and trade or hot wars.
- ***'Fake People' technology***. After the sale of the first AI-generated painting in early 2018, deep learning algorithms now generate portraits of non-existent people. The NVIDIA company has recently published the results of the work of a generative adversarial network (GAN) trained to generate images of people. The technique is based on an infinite collection of images of real faces; this is why a neural network recognizes and applies many fine details in its work. It can generate hundreds of faces with glasses, but with different hairstyles, skin textures, wrinkles and scars, and add age signs, cultural and ethnic features, emotions, moods or effects of external factors, such as wind in the hair or an uneven tan. Today, neural networks are incomparably better and generate faces in high resolution. They can easily produce, for example, an image of a non-existent illegitimate child of a celebrity, with a perfect family resemblance, as a provocation.

● ***Agenda setting and amplification***. Studies indicate that bots made up over 50 percent of all online traffic in 2016. Entities that artificially promote content can manipulate the "agenda setting" principle, which dictates that the more often people see certain content, the more they think it is important. Reputational damage done by bots during political campaigns, for example, can be used by terrorist groups to attract new supporters or organize assassinations of politicians.

● ***Sentiment analysis*** is a class of content-analysis methods used in computational linguistics to identify emotionally loaded words in texts that reveal the author's opinion of the topic. Sentiment analysis is done on the basis of a wide range of sources, such as blogs, articles, forums, polls, etc. This can be a very effective tool in PW.

● AI, machine learning and sentiment analysis make it possible to ***predict the future by analyzing the past*** — quite a holy grail for the financial sector or government planning agencies. But various state and non-state actors can potentially use this possibility for MUAI. Particularly important are ***prognostic weapons***: predictive analytics methods based on big data and AI, which make it possible to correct the future from the present in one's own interests and contrary to the objective interests of the target.

● It can be imagined that due to a combination of psychological influence techniques, sophisticated AI systems and big data can produce rather soon the **pseudo reality, the Matrix** which can be much more efficient tool of control of targeted audiences than now.

Finally Prof. Pashentsev analyzed several types of MUAI threats (including the sphere of IPS) during the possible transition from Narrow AI to General AI and further to ASI. "Unlike hypothetical aliens, General AI will be an intelligence with historical, scientific, philosophical and cultural roots in modern human civilization. It will be an intelligence that will develop faster and better than any of the past human generations. But it will have its origin in us. It is another matter that this intelligence may not want to put up with several negative and dangerous manifestations of modern human society that are dangerous to humans and the entire planet, such as the threat of world war, environmental pollution and other growing problems", clarifies Evgeny Pashentsev."General AI will not be a product of mankind in general, but specific people. It may be produced in a laboratory controlled by anti-social, reactionary or militaristic circles".

After the seminar there was a discussion between Russian researchers, members of GlobalStratCom strategic studies associations working at different Russian universities and academic institutions and the UCT Department of Political Studies leadership on possible ways of future academic collaboration. The interest for research of BRICS countries social and political development was expressed by both sides.

During their stay in Cape Town Russian scholars visited the Museum of Contemporary Art Africa (MOCAA) which have enough exhibits close to the topic of international psychological security.

Fuelled by a $38 million renovation project, a decrepit grain silo complex in Cape Town, South Africa has been transformed into the largest contemporary art institution on the continent, it opened its doors to the public in 2017. The museum offers an expansive, impressive space devoted to African art and artists—but it has been dogged by controversy since its inception. MOCAA is located on the V&A Waterfront, a popular cultural hub that overlooks the Atlantic Ocean. More than 100 galleries, spread out over nine floors, exclusively showcase the work of 21st-century. MOCAA has not been uniformly embraced by South Africa's art community. One point of contention for MOCAA's critics is the racial makeup of the museum's top-ranking players. In spite of the controversy, many African artists are cautiously optimistic about the new museum.

Port Elizabeth

In Port Elizabeth Prof. Evgeny Pashentsev and Dr. Olga Polunina were invited to visit the Nelson Mandela University, the Department of Political and Conflict Studies March 7 by the kind invitation of Prof. Lyn Snodgrass, the Head of the Department.

Nelson Mandela Metropolitan University (NMMU) opened on 1 January 2005, the result of the merging of the PE Technikon the University of Port Elizabeth (UPE) and the Port Elizabeth campus of Vista University (Vista PE). This union of three very different institutions came about as a result of government’s countrywide restructuring of higher education – intended to deliver a more equitable and efficient system to meet the needs of South Africa in the 21st century. On 20 July 2017, Nelson Mandela University was officially renamed: the only university in the world to carry the name of Nelson Rolihlahla Mandela.

Nelson Mandela University (NMU)

The Department of Political and Conflict Studies is focusing on democracy, conflict and socio-economic inequality issues, which is a good starting point for collaboration with GlobalStratCom strategic studies associations.

The Department did all possible to organize a workshop March 7 on “Artificial Intelligence and Trends in the Global Security Arena”. But the university leadership announced that lectures would not take place on Thursday due to the protests over student funding and accommodation. A public lecture with Professor Evgeny Pashentsev, a communications specialist, was also cancelled and staff were encouraged to work off-campus. But hopefully the ties and collaboration of the Department of Political and Conflict Studies with Russian researchers on strategic studies to be developed in future.

Johannesburg

The Russian researchers March 10-11 took part in cultural programme visiting Soweto ("South Western Township"), a suburb of Johannesburg, South Africa, became one of the historical symbols of the struggle against apartheid and Apartheid Museum.

All the trip demonstrated the rising need for collaboration with the researchers of South Africa on study of different issues of strategic communication, including the prospects for joint research of BRICS strategic communication and the issues of MUAI.

Photos are available on following e-addresses:

https://photos.google.com/share/AF1QipOHcVTHBtyCOC_Y9dQjOP5m1_ZzdRmy1D7hwoyqbNGCnyy60pfz-CbkFVopzpjC9Q?key=NzlNU3lUQ281bVZsYVpiSG5OUDBOaTRpclI0ZTh3

https://cloud.mail.ru/stock/144tjwz1cgd3W5gt6qih4pLY

See more: Russian Researchers on Strategic Communication in South Africa//**Asociației Geopolitica Estului (A.G.E.). 22.03.2019.**