Journal of Computer Virology and Hacking Techniques (2020) 16:257–258
https://doi.org/10.1007/s11416-020-00372-w

EDITORIAL

Editorial

Eric Filiol[1]

Published online: 1 November 2020

It is with great pleasure that I see this special issue devoted to Russian research in cryptology and information and systems security achieved and published. A longstanding project, the aim was to contribute to raising awareness of Russian research activity, which is unfortunately not sufficiently known in the Western world. Russian science, a prisoner of a tongue little known and unfamiliar to the rest of the world, is nevertheless extraordinarily rich, powerful, rigorous and refined. Science and research should make it possible to better understand our universe and nature—a mathematical function or an algorithm are ultimately natural objects that we are trying to understand. Above all they should offer a common language for all humanity. However it is sad to note that they still remain too compartmentalized by political considerations that separate rather than bring people together. I am equally happy and grateful to Drs. Ekaterina Griboedova and Vasily Shishkin, two eminent cryptologists, members of the Russian Technical Committee "Cryptography and Information Security" (TC 26) of the Russian governmental standardization organization (Rosstandart, GOST R) for accepting our invitation to write an article on the process of standardization in cryptology in the Russian Federation.

A French MP, Mr Bernard Carayon, Rapporteur on defense issues at the French National Assembly, claimed at the SSTIC 2004 conference that a country's power lies in its ability to impose norms and standards. With the implicit corollary that the weakness of other countries lies in the imposition of foreign standards. Alas, the whole drama of Europe is summed up here. Almost all the security standards that Europe uses come from the United States and in the near future some of its standards will probably also be Chinese. The agenda—economic, strategic, political—of these two countries in no way coincides with that of European countries and the rest of the world. In the field of security and especially in the field of cryptology—the most sensitive part of security—the situation since the end of the Second World War can be summed up as the control of cryptography by a handful of countries in the very closed club of the AUSCANNZUKUS, better known as the "five eyes". This control is enforced through regulations such as former CoCom, ITAR regulations and nowaday the Wassenaar agreement. The Hans Bühler affair in 1995 and the revelations of Edward Snowden since 2013 have shown that using technologies provided by the adversary is dangerous. The timid and recent research in the field of backdoors (may them be at the mathematical, software or hardware levels) shows that the security of a Nation State, and therefore its power, lies in its sovereignty and its technological independence. And for this, a rich and active science is needed.

From then on, the Russian standardization process, summarized in the article by Ekaterina Griboedova and Vasily Shishkin, shows all the modernity of the Russian Federation in a process of preserving its cryptologic sovereignty. The cryptographic algorithms of the GOST standards have, since 1989, shown great maturity and provided an alternative vision in current "standardized" cryptographic thinking. I hope that Europe will do the same and that cryptology science will be able to express all its richness through the birth of several interoperable international standards. The security of information and systems necessarily depends on the variety of algorithms and not on the uniformity and hegemony of a single algorithm. From this point of view, IANA's move towards this plurality of cryptographic algorithms within the TLS cipher suite is to be welcomed and demonstrates a hopeful intelligence. Variety offers freedom and sovereignty.

I therefore give readers the pleasure of discovering this special issue and perhaps, I hope, the desire to know this formidable scientific country that is the Russian Federation better.

This project would not have seen the light of day without the benevolence and trust of the publisher Springer. For 16 years, he has supported and accompanied this research journal with unfailing loyalty. This editorial allows me to thank him from the bottom of my heart and in particular all those who have worked so hard to produce this special issue and their continued support for the journal: Adam Ralph, Shanthakumar Kulaseka and Kaaviya Haribabu. I would also

✉ Eric Filiol
eric.filiol@univ-ubs.fr

[1] ENSIBS, Cyberdefense Dept., Vannes, France

like to thank Alisa Koreneva and Professor Fomichev, guest-editors for this special issue. They have done an outstanding job of selecting, managing the reviewers and proofreading the articles. Except to be behind the scene with them, it is impossible to imagine what such an activity involves in terms of effort and rigor. In addition to their competence and scientific quality, I would like to thank them for their kindness. It is a quality rare enough these days to underline it.

Finally, a project is the result of encounters, and these encounters can only take place thanks to people of good will. I would like to thank two in particular who have worked to put the right people in touch: Alexander Istomin and Grigory Marshalko. I know how humble they are, but I would be remiss if I forgot them.

I wish you all a pleasant reading of this special issue devoted to the Russian research in cryptology and information and systems security.