M.S. Gusman[1]

NEWS AGENCIES AND TODAY'S INFORMATION CHALLENGES

At the moment, there are more than one hundred big news and information agencies operating all over the world. My personal many years' experience in the TASS Russian News Agency, regular meetings with the managers of world news media and participation in international forums allow me to say that all news and information agencies encounter the same challenges in their activities. One of the most significant challenges is growth of cybercrime, which remains an undeniable threat to collective security. In 2016, about 1.5 mln cyber attacks were registered all over the world, to say it differently – more than 4,000 per day.

The current level of information networks' development allows to speak about formation of the one common information space, in which suppliers and consumers of information interact in real time. The increasing speed of data transmission and structural development of information networks, on the one hand, incessantly make the information transmission and processing process quicker and quicker. But on the other hand, the growth of influence and expansion of information networks' scope make them more and more attractive for criminals.

The Internet space is more and more often used by terrorist organizations as a venue for advocating and promoting extremist views and even enlistment in their ranks. It's not infrequent that social media with big numbers of subscribers and at the same time not always capable to provide control over the posted content, become such venues. Special features of social media providing everyone who wishes it an opportunity to speak up, independent of his/her competence in the issue, thus helps increase of tension in the information space.

[1] First Deputy Director General of TASS Russian News Agency, Professor, Merited Man of Culture of the Russian Federation. TV and radio presenter. The author of TV series "The Formula of Power" (more than 350 exclusive interviews with world leaders since 2000). The author of books, scripts for TV films and programs. Vice-President of the World Congress of news agencies, the Representative of Russia in the International Programme for the Development of Communication (IPDC). Laureate of State Prize of the Russian Federation and Moscow Government Journalist Prize. He was awarded with the orders "For Merit to the Fatherland" (4th class), Order of Friendship, Order of Honor.

Modern news and information agencies being an important component of global information networks are also in danger of attacks by cybercriminals. However, in this case, it's first of all leaked fake provocative information. The role played by news and information agencies in formation of the news picture of the world is extremely great. News and information agencies promptly generate information and deliver it to mass media, being one of the key links in efficient functioning of the world community.

And publication as a result of hackers' attacks on agencies of misleading information becomes even more dangerous. In the best case, criminals will confine themselves to just cyberinvation, in the worst case the placed information may act as a catalyst for an international conflict. Already in 2009, Hamadoun Touré, Secretary General of the International Telecommunication Union, the specialized agency of the United Nations, said that in case of World War Three it would take place in cyberspace.

As it is well-known, leaked fakes are capable to have a negative impact on news agency's reputation and even destabilize political environment. A question arises: how is it possible to resist cybercriminals? First of all, security of the global information space is unthinkable without working out provisions for this sphere. Currently, the world community is lacking a common program for resisting cyber threats. The necessity to adopt such a program is becoming more urgent every year. It's noteworthy that Russia presented such an initiative to the UN and the USA already in 1998.

Nevertheless, a number of programs are operating at the level of international organizations and certain states. Thus, in 2001, the Convention on Cybercrime of the Council of Europe (also known as the Budapest Convention) was signed in Budapest. In 2011, Russia, China, Tajikistan and Kazakhstan ratified the agreement on cooperation in information security within the framework of the Shanghai Cooperation Organization.

Russia is one of the cybercrime resisting centers. On December 5, 2016, the Presidential Edict approved the Information Security Doctrine of the Russian Federation, in which combating cyber threats is closely connected with national security. The draft Strategy for Information Society Development in the Russian Federation in 2017–2030 is under discussion, special attention in it is paid to security and trustworthiness of information. On January 22, 2017, Agreement on cooperation in ensuring security in information and communication technology use signed by Russia and India came into force.

Besides implementation of respective programs at the state level, it's necessary for news and information agencies themselves to work out means protecting from hacking. Attraction of IT experts and setting up specialized departments in agencies will help creation of up-to-date protection means blocking cyberinvation attempts and providing safe data transmission. At the same time, it is required to constantly advance systems controlling published content. The speed of data transmission makes news and information agencies quickly monitor the materials looking for inaccuracies and falsifications. Taking into account fake leaking, agencies have to think jointly about some "hot data key", prompt verification of information.

Understanding cybersecurity as an inalienable part of corporate culture is of no small importance either, it supposes personnel training in the safety rules for working with information. In some cases criminals may use internal accounts of agency's employees for access to corporate information.

Today's news or information agency is unthinkable without a proper website. Materials published on news websites are immediately spread all over the world. DDoS-attacks' becoming more frequent and leading to prolonged failures in operation make us maintain up-to-date protection of our news websites.

Finally, as numerous examples above show, it's necessary for news and information agencies to pay special attention to security issues when working with social media, especially vulnerable to hacking. This includes elementary measures as complex passwords for accounts and established communication channels with respective service departments with which we cooperate.

I am sure that using the methods described above and observing world standards for information control and security, news and information agencies will be able to successfully resist all challenges launched against them by the not simple and rapidly changing situation in the world.