RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International and of the Centre russe d'études politiques.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 10 (202), vol.12. October 2013

October 11, 2013

Oleg Demidov reports from Moscow:

EDWARD SNOWDEN'S TEN BOMBSHELLS THAT SHOOK THE WORLD:

HOW RUSSIA AND ITS PARTNERS WILL RESPOND

ANNOTATION

For quite a short period of time starting from July 2013 the fugitive American intelligence analyst Edward Snowden has revealed huge amounts of classified information about America's and Britain's clandestine surveillance and intelligence gathering in the Internet and other communication networks.

Oleg Demidov, head of the PIR Center program on International Information Security and Global Internet Governance, has collated the information disclosed by Snowden, and highlighted the parts of it that have had the most profound effects on the leadership of Russia and its partners, as well as on the international community. He has concluded that the information bombshells dropped by Snowden could trigger some very serious decisions and initiatives in Russia and internationally.

EDWARD SNOWDEN'S 10 BOMBSHELLS

1. The Bullrun program: a comprehensive set of measures to circumvent Internet encryption protocols.

Starting from 2000, the developers of encryption tools in the United States have been engaged in *half-voluntary, half-forced* cooperation with the U.S. National Security Agency (NSA) and other American secret services. Yielding to pressure or bribery, the developers have been leaving various hardware and software *backdoors* in their products used by IT services, banks, and other clients - including foreign ones. Essentially, we are talking about the security services pressuring commercial companies into inserting fundamental vulnerabilities into their software, and then making use of those vulnerabilities. As part of the *SIGINT* program, which is related to *Bullrun*, the NSA has been spending up to 250 million dollars every year to bribe companies into leaving backdoors in their commercially marketed software products.

No reliable encryption products means no reliable services and, as a result, no confidence in the Internet. This does not merely affect the United States or the numerous products and services targeted by the NSA. This has a global, planetary effect.

Clearly, the methods used by the NSA as part of *Bullrun* violate the key principles and undermine the basic technology of Internet security. That is why they pose a fundamental threat. As Bruce Schneier, a world-famous cybersecurity expert, has put it, "the U.S. government has betrayed the Internet".

2. It is quite possible that fundamental vulnerabilities in the Advanced Encryption Standard (AES) have been exploited since 2002. AES is a block encryption algorithm and a U.S. national encryption standard widely used all over the world.

In Russia, many services which are not required by law to use the Russian national encryption standards (part of the GOST standards system) rely on products based on the AES. The situation is very similar in the rest of the world, with the exception of China and a handful of other countries. Internet banking systems, social networks, online chat rooms, corporate networks, and email – all these key services rely on AES encryption. In addition, the NSA has had some success with breaking the SSL protocol, which is fundamental to the security of most Internet communications. There is an integrated database that enables matching encryption keys to secured data to be produced instantaneously. According to Snowden, the new priority targets for the NSA are Virtual Private Networks (VPN) and 4G security technologies. The U.S. secret service's plans for 2013 include the insertion of *backdoors* in widely used computer chips. In other words, the agency is moving on from software methods of circumventing encryption to hardware methods.

3. Tracking VISA payments by private individuals and wire transfers via the SWIFT interbank payments system: the Follow the Money program and the Trackfin database.

As part of this particular program, records have been accumulated for a total of 180 million operations, of which credit card operations by private individuals accounted for 84 per cent. In 2012, if not earlier, the NSA gained access to the *SWIFT* system of bank transfers, which is used for 3 billion wire transfer operations every month. The geographic priorities of this program are Africa, the Middle East, and Europe. *VISA* itself denies any involvement; in other words, in this particular case the payments system has not been co-opted by the secret services; rather, it has simply been hacked. Of course, had it actually been co-opted, the company would not have admitted it anyway. Be that as it may, the situation is a serious blow for international financial security.

4. PRISM – large-scale clandestine gathering of information transmitted via electronic networks.

The *PRISM* program, which was launched in 2007, enables the U.S. government to download secure information from the servers of such U.S. internet giants as *Microsoft, Yahoo!, Google, Facebook, AOL, Skype, YouTube, Apple, PalTalk,* and others. That information is usually being accessed with the knowledge of these Internet companies, which means that they are closely affiliated with the U.S. secret services. The PRISM program gives the NSA,

the CIA, and the FBI access to private email communications, video and voice chats, video recordings, photos, other information stored on hard drives, VoIP traffic (internet phone calls), all kinds of computer files transferred over the Internet, online video conferences, logins and passwords, messages and activities in the social networks - the list goes on and on. The program also keeps records about phone calls – both domestic and international - made by the subscribers of the largest U.S. mobile phone companies.

5. XKeyscore – a universal data search and analysis tool.

Here is just a short roundup of what the *XKeyscore* program can do. By typing in an *email* address, the operator can gain access to the contents of the mailbox, the contacts list, and the IP address used to access the email box. By typing in an IP address, the operator can see the list of all the websites visited from that address, all the logins and queries entered from it, and all the documents viewed. He can also break into accounts on social networks and intercept chatroom messages. The program keeps records about all connection sessions, intercepts and stores all textual communications logs, identifies the nationality of the subject based on the contents of intercepted email communications, and highlights any anomalies in communications, such as the use of PGP-type encryption programs to browse the Internet. The program can even identify the original author and source of the documents copied or transferred via the Internet. It relies on 700 servers, most of them physically based in the U.S. embassies and consulate offices in other countries; there is a server in Moscow as well. Future plans for this program include new capability to intercept VoIP and geo-positioning (GPS) data.

One particular VoIP service, *Skype*, deserves a separate mention. The Kremlin is seriously considering the FSB proposal to ban *Skype* in Russia because the Russian secret services do not have access to the original encryption key used for *Skype* VoIP traffic. According to some reports, the problem was partly resolved in 2011, when *Skype* was acquired by *Microsoft*, which is more inclined to cooperate with the Russian authorities – but the issue still remains on the agenda. As far as Russia is concerned, arguments to the effect that *Skype* is controlled by the NSA and the British secret services are an excellent justification for granting the Russian security agencies access to *Skype* traffic as part of official, legitimate and systemic arrangements, rather than some unofficial and extrajudicial mechanisms. The alternative is to restrict the use of *Skype* in Russia.

6. Systemic offensive cyber operations by the U.S. secret services against networks in foreign countries, including China, Iran, North Korea, and Russia.

According to the classified budget of the U.S. secret services revealed by Snowden, 4.3bn dollars have been allocated to finance operations in foreign networks in 2013. In 2011, some 231 such operations were *proactive*, i.e. offensive. Interestingly, apart from preventing intrusions into U.S. networks, these operations also pursue the purpose of "preventing nuclear weapons proliferation". That confirms once again the origins of such viruses as *Flame*, *Gauss*, *Duqu*, and *Stuxnet*, which primarily targeted Iran. In and of itself, this is nothing new; the surprising thing here is how much money is being spent on this program. The axiom about *cheap cyberweapons* has been circulating since 2010; how many products and operations like these can be financed for one billion dollars a year? The size of the U.S. secret service's budget suggests that the range of instruments developed to stifle Iran's peaceful nuclear program is much wider than previously thought. And since spending on this particular item continues to grow, Iran is clearly not the only country being targeted.

7. Numerous operations by the NSA and Britain's Government Communications Headquarters (GCHQ) to eavesdrop on senior foreign officials and delegations, including the operation to intercept secure communications via satellite between Dmitry Medvedev and Moscow when the then Russian president was staying at the Russian embassy in London during the G20 summit in April 2009.

The eavesdropping operation was conducted from the Menwith Hill spying station; its results are unknown. Also in 2009 the U.S. and British secret services broke the encryption used by *Blackberry* smartphones to intercept phone calls and messages between the G20 delegates.

Similar operations have been conducted against foreign delegations, government agencies, and embassies of many countries, including those which believe themselves to be Washington's allies. Such practices came as a particular surprise to Latin American countries, including Mexico and Brazil; the NSA eavesdropped on their presidents' phone calls and intercepted their email messages. There was talk of cancelling the meeting between Brazilian president Dilma Rousseff and Barack Obama scheduled for October 2013. This could be just the beginning of a snowball of complications in U.S. relations with other countries; that snowball will continue to grow if Snowden makes new damaging revelations.

8. The GCHQ's Tempora program: Mastering the Internet and Global Telecoms Exploitation.

This particular program collects vast amounts of information about phone calls and Internet traffic. The data collected by the program can be stored for up to 3 days; the metadata is stored for up to 30 days. The program records phone calls, email exchanges, messages and personal data on *Facebook*. In 2011, some 200 broadband lines, each with a 10 Gbps capacity, were used to obtain, process, and store information as part of the *Tempora* program. The British government is now planning a tenfold increase in that capacity. The list of the targets of this intelligence-gathering operation has not been disclosed; experts describe it as "endless".

For Moscow, the main conclusion that can be made from this unpleasant discovery is that in terms of their appetites and the scale of electronic surveillance, the British are not far behind the Americans.

9. A huge NSA surveillance program targeting commercial companies in Brazil and several other countries.

The NSA has been systemically intercepting phone calls and email exchanges by senior executives of the Brazilian oil giant *Petróleo Brasileiro S.A.* (*PetroBras*). This particular episode has punched a major breach in Washington's main line of defense – mainly, its claims to the effect that "we have to spy for a noble cause, the war on international terrorism". Infuriated by this discovery, Dilma Rousseff rightly noted that "*PetroBras* is not a threat to the national security of any state". But the company certainly is a very large and strategically important part of the Brazilian economy, with a market capitalization of over 100bn dollars, gross annual revenues of 144bn, and an 80-per-cent share of Brazil's national oil output.

This is where the Americans have run out of any plausible arguments; the U.S. position regarding governments' conduct in the Internet clearly does not hold water. Spying against strategic economic entities has always been portrayed by Washington as one of the strictest taboos, and as a key charge against Beijing. The alleged Chinese threat in this area was used by Washington as a justification for ramping up the financing and size of the U.S. Cyber Command and similar cyber outfits in the U.S. armed forces and secret services. It is very symptomatic that since July 2013 the Americans have suddenly stopped accusing Beijing of cyberespionage and cyber attacks.

10. A joint program by the NSA and the GCHQ to fit submarine fiber optic cable infrastructure, including intercontinental cables, with hardware bugging devices.

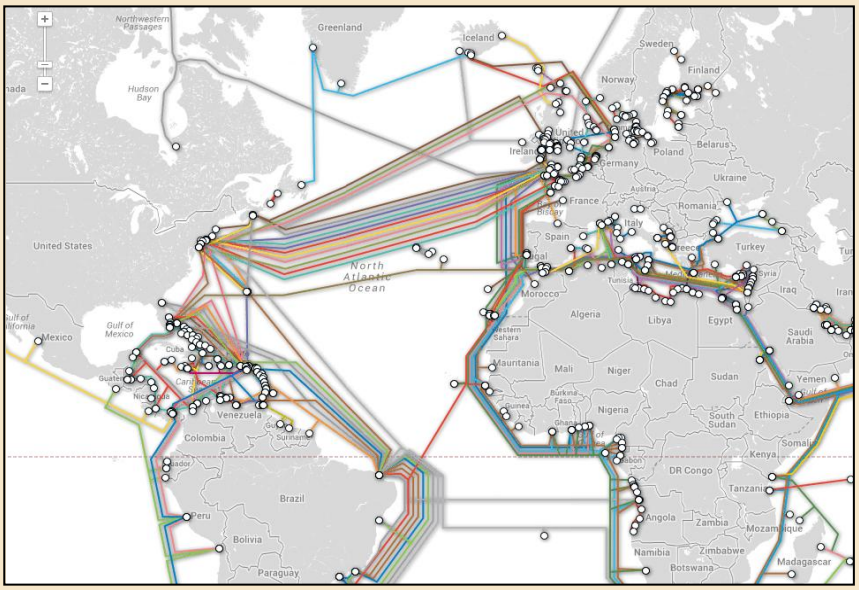
Britain is in a uniquely convenient geographical position to provide help to the Americans. More than a dozen submarine fiber optic cables that connect Europe and America pass through Cornwall, in the southwest of England. These cables account for about a quarter of the global Internet traffic (See Map 5 on p. 5). This is the biggest fiber optic infrastructure node of its kind in Europe. In particular, a large part of Internet traffic from Russia passes through that node.

Along with *Bullrun*, the insertion of hardware bugging devices to extract data directly from the submarine cables is an excellent example of the unfair game being played by Washington against its bitter rivals and close allies alike. Essentially, the United States and its British colleagues are exploiting their unique advantage, i.e. access to the underlying infrastructure of the Internet - the very infrastructure that is thought of as belonging to the whole world, just as the Internet itself is. As far as the spying software targeting various Internet services and applications is concerned, the leading international players

have a fairly similar capability. The NSA and the CIA are more or less evenly matched by hackers from Russia or China, and perhaps even from Iran as well. But in this particular case Washington and London leapfrog over all the upper levels of the Internet infrastructure and use the *trump card* of their unique access to the cables. The rest of the world is bound to respond by trying physically to neutralize that unfair advantage.

In this sense, Edward Snowden's disclosures are *a gift from above* for the proponents of stepping up the BRICS projects of laying its own long-distance submarine fiber optic cables. That includes the proposal to lay a 34,000 km long BRICS cable connecting all five countries, from Vladivostok in Russia to Fortaleza in Brazil, thereby reducing their dependence on the existing cable infrastructure (See Map 2). The launch of this project was originally scheduled for 2013, but there have been significant delays, and the new cable still remains on paper.

Map 1. Transatlantic submarine fiber optic cables



Source: TeleGeography. Submarine Cable Map 2013. http://submarinecablemap.com

Map 2. Proposed BRICS transcontinental fiber optic cable

Source: BRICS Cable. http://www.bricscable.com/network/

Considering the Russian and Brazilian reaction to Snowden's disclosures, the BRICS cable project appears a lot more likely to be implemented. The financing will probably come mainly from Brazil or Beijing rather than South Africa, which used to be the project's key proponent.

***To summarize all of the above:** The United States (London does not, after all, seem to play a key role here) has made a serious investment into maintaining its superiority in the Internet. That applies to every level of the Internet infrastructure, from cables and chips to VoIP services and social networks. In and of themselves, none of the facts revealed by Snowden seem very surprising or shocking. But taken all together, they have brought on an irreversible shift in the international community's perceptions. No-one will be able to convince Dilma Rousseff any more that the NSA is not listening in on her mobile phone calls. No-one can now give the FSB or the Russian Duma plausible assurances that the NSA is not reading Russian officials' Gmail correspondence, or that the British are not sifting through Russian Internet traffic passing via Cornwall. Finally, no-one can now persuade PetroBras that the motives of the American secret services are limited to national security, and have nothing to do with economic competition.*

The genie is now out of the bottle, and Snowden's disclosures have put more wind in the sails of those advocating the concept of digital sovereignty. That concept is especially popular in the BRICS countries and among the other giants of the developing world. The repercussions of these disclosures will not die down any time soon. The twists and turns of that story, and Snowden's current status, mean that no-one can be sure whether that *weird guy* knows the whole truth, or whether he has actually told everything he does know. The facts he has already revealed are bound to look like the tip of the iceberg of *Anglo-Saxon digital imperialism*. Edward Snowden is not a tectonic plate that will push the developing countries towards sovereignty on the Internet. But he is an ideal pretext and catalyst for these processes, and his contribution has been extremely timely.

HOW WILL RUSSIA RESPOND?

Russia has been campaigning against the *unfair world order* in the Internet since 1998. It has now found itself in an unusual but very pleasant situation. Previously, China and other Russian allies were hiding behind Russia's back. Moscow looked like a lone soldier on this battlefield. Now, however, Russia can take a breather and let the infuriated Brazil do some fighting, for a change.

An energetic response is already under way at every level. *PetroBras* has promised to spend an unprecedented 10bn dollars on beefing up its information security arrangements. Brazil has announced its intention to ask the United Nations to review the principles of global Internet governance. It has also proposed an initiative that is very similar to proposals made in July 2013 by members of the upper chamber of the Russian parliament: namely, to make it compulsory for the transnational IT corporations to keep the servers that store personal data of any third country's citizens on that country's own territory. It has also become more likely that Russia and Brazil will finally ratify their agreement on cooperation in the area of international information security, which was signed back in 2010.

What other consequences are likely to follow? In Russia itself, *Google* and *Facebook*, which were the first to come under a barrage of criticism by Russian lawmakers, will probably face growing pressure. We can also expect tighter regulation of VoIP services in Russia; new rules making it compulsory for Russian businesses, government agencies and organizations to use Russian national cryptography standards; more energetic efforts to develop a secure national computer operating system; new regulations regarding the social networks and the use of email by government agencies; etc.

Internationally, we can expect a new crusade by Russia and its BRICS allies against ICANN and the multi-stakeholder approach, with demands to make Internet governance part of the UN remit. The battlefields will include the Plenipotentiary Conference of the International Telecommunication Union in November 2014, and the WSIS+10 process in 2015. The first signal can be sent in October during the Internet Governance Forum on Bali, for which the Russian delegation is busily preparing. Also, it is not hard to envisage projects to lay new submarine cables piggybacking on the big Russian projects to lay submarine pipelines, thereby connecting Russia with its BRICS partners.

Does Russia possess the necessary resources and technologies to reach the goals at the end of this difficult path? I believe that it does. Will all the aforementioned strategies make it more difficult for the NSA and the GCHQ to target Russian networks, if these strategies are actually implemented? I do not doubt that they will. But will such strategies serve the interests of the Russian IT sector, and the Russian national interests as a whole? That is a very contentious issue. Completely subordinating regulation of the IT sector to the security imperatives could potentially become a heavy burden and slow down that sector's growth. As Russia is clearly entering a period of stagnation or even depression in 2014, such a turn of events could leave the Russian economy without what has been one of the most powerful and reliable engines of its growth in recent years – an engine that is not dependent on exports of raw materials.

If that is allowed to happen, the blame will certainly lie neither with the NSA, nor with Edward Snowden.

The author of this article is Oleg Demidov, head of the PIR Center Program on *International Information Security and Global Internet Governance*

Editor: Julia Fetisova

Moscow-Geneva, October 2013

Excerpts from the Membership Terms and Conditions at the Trialogue Club International

3. Club members' rights

[…]

3.1. Individual members of the Club have the right to:

3.1.3. Receive one copy of the Russia Confidential exclusive analytics bulletin by email, in their preferred language (Russian or English). Under the rules of the Club, the bulletin may not be made available to third parties.

[…]

3.2. Corporate members of the Club have the right to:

3.2.3. Receive two copies of the Russia Confidential exclusive analytics bulletin by email, in their preferred language (Russian or English) or in both languages, and to make the bulletin available to other representatives of the corporate club member. Under the rules of the Club, the bulletin may not be made available to third persons who are not members of the Club.

[…]

4. Club members' responsibilities

4.1. All current members of the Club have the following responsibilities:

4.1.6. Not to share materials of the Russia Confidential bulletin they have received, as well passwords to the Club section of the PIR Center website, with individuals and/or entities who are not members of the Club.

[…]

6. Russia Confidential

6.1. The Russia Confidential exclusive analytics bulletin is issued by the Trialogue Ltd at the commission of PIR Center for personal use by Club members only.

6.2. The bulletin contains concise and exclusive analysis of problems pertaining to international security, as well as foreign and domestic policies of Russia and CIS states, written specially for Russia Confidential by PIR Center staff and invited experts.

6.3. Materials published in the bulletin should be treated as confidential for at least 30 days since the date of publication. During that period they may not be quoted or made available to persons or entities who are not Club members.

6.4. After a period of at least 30 days since the date of publication the Trialogue Ltd may choose to lift the exclusivity and confidentiality requirements for some of the materials published in the bulletin, in which case they may be reprinted in other PIR Center publications and quoted by Club members.

6.5. The bulletin is sent to Club members by email on a monthly basis, in English or in Russian, depending on the individual club member's preference.

6.6. Upon request, Club members can also receive a hard copy of the bulletin in their preferred language.

Dear Members of Trialogue Club International,

Trialogue Club celebrates its 20th Anniversary in 2013!

*Trialogue Club International has become a unique informal community of leading diplomats, experts and industry captains. In 2013 members of the Club will be offered: a chance to take part in **five** meetings with leading Russian and foreign experts on international security; **four** issues of the Security Index magazine; **12** issues of the Russian Confidential exclusive analytics bulletin; **free** participation in various PIR Center academic events; and **several pleasant surprises** for our permanent members.*

As you know, we are always very happy and appreciative when current members of the Club recommend Club membership or participation in our events to their friends and colleagues. Such a recommendation means an automatic membership offer. In addition, we are offering two kinds of reward for bringing a new member to the Club; the details are outlined below.

I look forward to seeing you and your colleagues at Trialogue Club meetings in 2013!

Sincerely yours,
D.V. Polikanov
Chairman of Trialogue Club International

Rewards for bringing a new member to Trialogue Club International

Option 1 – Membership fee discount for the next period	
5%	for 1 new individual Club member
10%	for 1 new corporate Club member
10%	for 2 new individual Club members
15%	for 3 new individual Club members
20%	for 4 or more new individual Club members
20%	for 2 new corporate Club members
30%	for 3 new corporate Club members
35%	for 4 and more new corporate Club members

Option 2 – Lump-sum compensation in cash	
100 USD	for 1 new corporate Club member
200 USD	for 2 new corporate Club members
300 USD	for 3 new corporate Club members
500 USD	for 4 and more new corporate Club members