Information & Security: An International Journal

Milan Sekuloski, v.34:1, 2016, 69-90 https://doi.org/10.11610/isij.3406

SECURITY SECTOR REFORM WISDOM FOR CYBER SECURITY INSTITUTION BUILDING: THE CASE OF SERBIA

Milan SEKULOSKI

Abstract: The following article considers cyber security as an integral part of security sector reform (SSR), trying to identify some of the lessons learned from Serbia that can help when establishing a credible cyber security system. Serbia represents a telling example, as it is a country that has been undergoing significant SSR, implemented in both post-conflict and developmental context. Having in mind that Serbia is at the beginning of building its cyber security system, the article provides guidance on how to best integrate lessons learned from other SSR processes. The first part discusses the inter-linkage between SSR and cyber security institution building. The second part offers examples of initiatives implemented in Serbia during 2015, with an aim to illustrate the importance and benefits of the holistic approach to cyber security institutions building in line with the core principles of SSR. Examples present a point into an OSCE Mission project which demonstrates the importance of synergies and of a holistic, multi-stakeholder approach for effective building of functional cross-sectoral networks that can contribute to building national cyber security capacity. For its part, the cyber security capacity building initiative of government witnesses how SSR processes and actors promoting accountability can positively influence the efficiency of cyber security capacity building efforts. Another example presents how the first ever public hearing on cyber security in the Serbian Parliament was organised. It illustrates that the Parliament can be an effective starting point for a national debate on cyber security and a very efficient awareness raising tool.

Keywords: security sector reform, cyber security, cyber crime, institution building, multi-stakeholder approach, Serbia.

Cyber Security and Security Sector Reform

Security sector reform is built on the concept of human security, which was introduced by the United Nation's Development Programme (UNDP) in its 1994 global Human Development Report. Human security broadens the scope of the traditional notion of security, from territorial/state security to the security of people/individual and societal security. It calls for consideration of security through seven dimensions: economic, food, health, environmental, personal, community, and political.

The UNDP's list of human security dimensions is not exhaustive, and there are certainly various cross-cutting issues that need to be taken into account, such as some of global, and some of a more regional nature.

The trend of the definition of the notion of security's becoming more complex, and it may result in security provision being understood as one more function that it might be provided to the citizens not necessarily by the state, but rather by a functioning state managed network. This corresponds to Goldsmith and Eggers partnership theory on *governing by networks*: government executives are redefining their core responsibilities away from managing workers and providing services directly to orchestrating networks of public, private, and non-profit organizations to deliver the services that government once did itself.[1]

The states can provide preconditions for this kind of security only by implementing the democratic/good governance models of state administration. Good governance in security sector is essentially a state-centric concept. It is one which shares with the concept of human security a concern for the welfare and safety of individuals, groups and society. And more often suffers from a poorly governed security sector.[2]

Traditionally, the security sector was regarded as the armed forces of the government, i.e. the institutions possessing the government's monopoly over the use of force and restriction of civic rights. However, the extended understanding of the notion of security lead to the inclusion of other state and non-state actors among the security sector actors in a given society or a state. Figure 1 from DCAF/ISSAT's manual1 [3] illustrates this very well:

An internationally recognised way of achieving democratic governance over a security sector is the security sector reform (SSR). SSR will thus be regarded as a set of processes in a given society aimed at increasing the effectiveness and accountability of security providers. This is a common understanding, and it is accepted, *inter alia*, by the United Nations.[4]

This concept is fairly new, and has been introduced to describe the changes traditional security providers (predominantly, but not exclusively, state institutions) had to undertake to be able to adapt to the changing understanding of what security is (from traditional to human security), how it should be provided (adherence to good/democratic governance principles), and to whom (from state centric to people centric).

As for most reform policies, the context in which the reforms are taking place is of crucial importance. Bryden and Hänggi make a distinction of these contexts based on the key rationale for the reform, and divide them in three groups: [5]

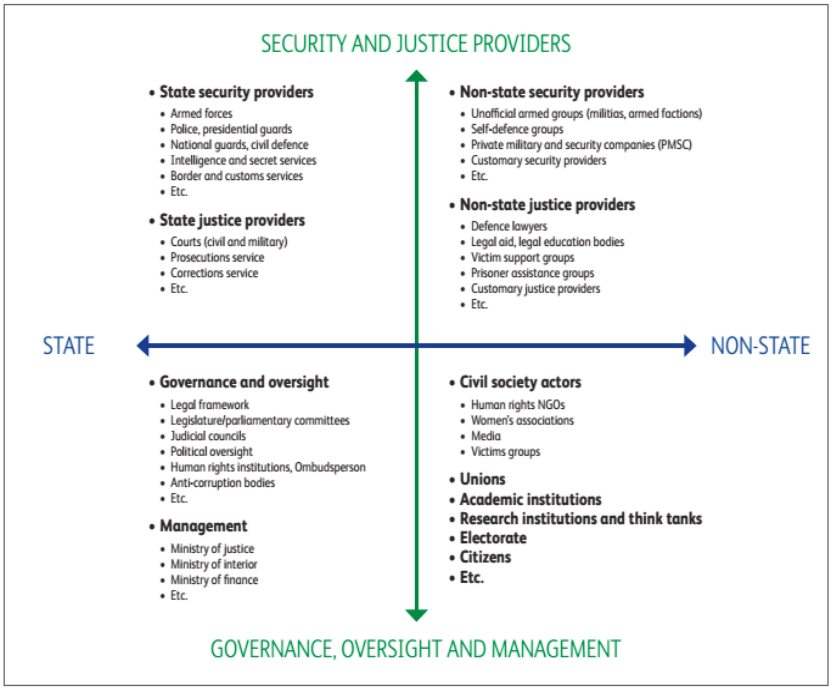

Figure 1: Security Sector Reform (SSR).[2]

- the developmental context in relatively stable developing countries, where key rationale for the reform is the socio-economic development of that society
- the post-authoritarian context in countries with key reform driver being the transitioning of the political system, and
- the post-conflict context in countries engaged in enhancing the security situation by rebuilding the state after conflict.

Although all three contexts are applicable to the specific case of Serbia, however we will position it against the developmental background as it is applicable to any country from the region (and beyond). Additionally, it dominates the years following the 2008 global financial crisis, with most of the countries having defined the recovery of the economic crisis as their top policy priority, and having enforced hard austerity measures. Yet, Serbia is no exception to that. SSR is thus becoming increasingly relevant in the developmental context.

In addition, one needs to account for the important role of the internet in modern economies; securing the cyberspace is more important than ever. Cyberspace is un-

derstood as the realm of computer networks (and the users behind them) in which information stored, shared, and communicated online is certainly an important element of anyone's security today.[6] We argue that all of the listed human security dimensions have a cyberspace component, which is becoming increasingly important.

The use of modern information and communication technologies (ICT), and most notably the Internet, are influencing everyday lives of citizens in all countries of the world, including Serbia.[7] None of the proposed seven dimensions of human security, as defined by the UNDP's 1994 global Human Development Report, can be properly considered without considering how do ICT technologies affect it now, and more importantly, how could they affect them in the future.

As Singer and Friedman note, while cyberspace was once just a realm of communication and then e-commerce (reaching over $10 trillion a year in sales). Then it has expanded to include what we call *critical infrastructure*. These are the underlying sectors that run our modern-day civilization, ranging from agriculture and food distribution, banking, healthcare, transportation, water, and power. Each of these once stood apart but are now all bound together and linked into cyberspace via information technology.[6]

Hence, we can conclude that cyberspace is becoming increasingly relevant for ensuring security in a society. Consequently, SSR as an internationally recognized way (in both theory and practice) of improving human security must take into account the cyber dimension, i.e. cyber security.[8]

There are many definitions of cyber security.[9] For this article, we shall consider cyber security as a set of institutions and policies in a given country that work towards minimizing threats to human security [10] emerging from or related to the cyberspace.

Cyber security policies can thus be rightfully seen as part of security policies of a country, and both as part of a societal development agenda. Law enforcement agencies are adapting to cyber crime related challenges by creating special units that will deal with the cyber crimes, the militaries are formalizing new cyber defence units, and civil rights defenders are much more attentive to the issues of on-line privacy intrusion. Security sector has long time ago expanded to cyberspace.

Any discussion on reforming a part of security sector in the developmental context, as defined by Bryden and Hänggi,[5] must acknowledge the importance of linking development with security, emphasising the crucial role a well governed, efficient security sector plays in the provision of security, and as a precondition of sustainable economic development. Conversely, if poorly managed and governed, the security sector can act as a spoiler of development efforts.[11]

Although linking SSR and cyber security may seem as a pretty straight-forward issue, it does have one implication that is often overseen in the debates about cyber security, that is: the element of accountability must always be observed when considering the capacity building in the area of cyber security.

If not taken into account from the outset, it may lead to the build-up of uncontrolled centres of power in some parts of the state/security apparatus, or even the private sector. This significantly increases the possibility for misuse of power, even in well-established democracies. Snowden's revelations of mass surveillance programs by US government, as well as the numerous cases of similar revelations in other countries, demonstrate this very well.

As Buckland, Schreier, and Winkler note,[12] cyber security poses a number of specific challenges to the democratic governance of the security sector. They particularly highlight democratic oversight challenges deriving from the following:

1. Network complexity: a large and diverse number of state, private, international, and other non-state actors constitute the backbone of internet, core element of cyberspace;
2. Technical complexity: a highly technical nature of cyber security challenges and responses;
3. Legal complexity: cyber security poses complex legal questions related (among others) to the right to privacy and freedom of expression;
4. Heterogeneity of actors: both public and private actors involved in cyber security cut across agency boundaries and thus across areas of oversight mandates. The result is a large number of areas with none or inadequate oversight;
5. Mandate perceptions: government oversight bodies are concerned with the government agencies over which they have direct responsibility, thus leaving the private partners of governmental agencies out of the reach of oversight, even in cases where they are directly funded by, or work in close collaboration with those agencies;
6. Breaking of principal/agent bonds: the actions of every government agent are connected in a chain of responsibility, from principal to agent. These links are broken by the introduction of private actors and the creation of public private cooperation mechanisms.

However, there are also a number of features of the SSR that correspond to the challenges that the processes of cyber security institutions building and policy making are facing.

First, the necessity of holistic approach that acknowledges various actors, both as security service providers and recipients (i.e. the multi-stakeholder approach)

The internet is at the core of cyber security. Its decentralized nature, loosely defined governance structures and reliance on both state, and privately owned resources makes the multi-stakeholder approach essential for any debate on cyber security. Most of the democratic oversight challenges listed by Buckland *et al* are directly linked to this fact.[13]

However, this is not unfamiliar to security sector reform theory and practice. For example, OECD refers to a system of multi-layered security governance in the OECD Handbook.[14] Whereas, DCAF/ISSAT SSR manual describes SSR as a process that involves a host of different services provided by different actors, institutions and agencies by its very nature. Adopting a holistic vision of SSR requires understanding the interconnected nature of the various components of the security and justice sector.[15]

It is widely acknowledged that in order to achieve sustainability, any SSR effort should be observed in correlation with other efforts, and the overall governance reforms. For example, if not aligned with human resource management policies related to staff promotion and retention, any training effort has very high risk of being unsustainable. *This is equally true for police officer trained in forensics and then assigned to administrative position as for any government employee trained in network security who moved to the private sector for a more competitive salary.*

Second, requirement of a wide range of skills and specific, not widely accessible knowledge

A successful SSR process is critically reliant on experts in specific reform areas, such as policing, defence, intelligence and local government but also in relevant cross-cutting issues, such as gender and human rights; technical expertise in areas as budgeting, logistics, communication and information technology systems, strategic management and training; experience in change management, including the leadership and communication skills to guide institutional, organisational and managerial reform processes in complex environments; and programme management skills – resource management, planning, reporting and coordination.[16]

Computer emergency response teams are at the heart of any cyber security system. They need to have not only sophisticated (and often very expensive) technical training, but also management, and people skills that would enable them to establish efficient teams and working relations with a variety of stakeholders. Namely, they are cooperating mostly on the basis of stakeholders' good will (in contrast to formal obligations deriving from legislation or contracts).

Third, the need for secrecy, opposed to accountability and privacy

Aside from the fact that clandestine interception of communications is one of their core activities, intelligence services are in many ways faced with the challenges inevitable for any institution dealing with cyber security:

- In order to perform their legitimate tasks, they need authorisation and knowledge to interfere in people's privacy;
- There will always be doubt and difficulty to explain the level of discretionary power necessary to perform these tasks;
- It is hard to communicate success rate to external public – failures are often obvious and visible to the general public, while successes are in fact often invisible, or visible only to a narrow group of persons and institutions.

In fact, intelligence services' work is legitimised indirectly, through the oversight bodies of the executive and the legislative branches of the government. This is still a challenging process, yet some lessons and experience are gained. It can be used to mitigate negative developments related to the establishment of cyber security bodies. The risks are, in this sense, even higher in the cyber security realm, due to the bigger involvement of private sector actors whose powers of intrusion might be even bigger than those of the national security and intelligence services, but without proper safeguards for misuse.

Fourth, there are scarce resources for reform projects, and they will not grow

The global economic crisis has had an impact on both developed and developing countries. In developing economies, such as those in the Western Balkans, it has increased social pressure and led to less public spending, including for reform initiatives that are not showing immediate effect (or at least not during a single election cycle).

It has also affected the developed economies, which are the main source of donor assistance programs for the developing countries' reforms (either through bilateral donations, or through international organisations and multilateral initiatives). It is thus reasonable to expect that the donor assistance will, if not decrease, certainly require a more efficient use of funds.

Other developments will also affect donors' prioritisation in deciding which reform programs to fund. For example: big influx of refugees and migrants to the European continent (which is unlikely to stop in the medium term). The complexity, and magnitude of the challenge the refugee/migrant crisis is putting in front of developed and developing countries (particularly those along the refugees/migrants' route, like the West Balkans countries) makes it highly unlikely that the donor countries will put

new development themes (such as building the cyber security system) high on the assistance agenda.

Development assistance will continue to exist, but there will be an increased demand for more efficient use of funds. This is already visible in EU's application of sectoral approach in programming donor assistance, aimed at increasing efficiency of usage of donor funding for desired reform results.

SSR is already on the agenda, and the support to these processes is part of commitments already made of both the EU and aspirant countries. Hence, securing funds for cyber security initiatives from those funds would be feasible on the grounds of supporting the SSR process.

Another important aspect is that cyber security may generate more interest on the part of the private sector (due to the organic link to internet/ICT businesses). This could open the way for private funding support for public reform efforts, either as an expression of corporate social responsibility or through public private partnerships. This may, to some extent, also benefit the SSR, in at least two ways:

- If successful in the realm of cyber security, it may encourage the use of public-private partnership models in security sector and governance reforms;
- Cyber security is cross-cutting many other development policies and sectors, and can indirectly help their better coordination with security policies.

Fifth, there is evident need for increased effectiveness and accountability

Figure 2 below shows the number of countries that have adopted a cyber security strategy. Thus, it is illustrating which states could have consistent cyber security policies and institutionalised answers to threats to their citizens coming from cyberspace.[17] Having in mind the theory and practice of implementing strategic documents in the public sector, it would be interesting to see how many of these strategies are successfully implemented. This is something which the map presented bellow does not show. However, what is evident from the map is that only Western Balkans (WB) country with such a strategy is Montenegro.[18]

Besides the fact that the vast majority of countries (of the Western Balkans) do not have credible cyber security policies and institutions, the large disparities in terms of both technological capacities and legal frameworks between the states that did adopt cyber security strategies implies that their experience cannot be directly transferred to these countries.

Moreover, the public and expert debate in the countries of the WB region is dominated by questions of effectiveness: experts call the governments to invest more resources into this area, and a call for increasing the public awareness on the im-

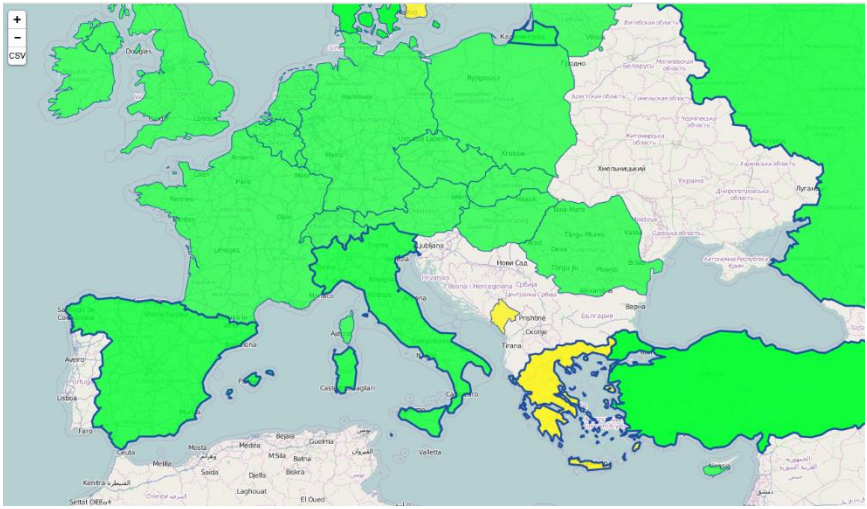

Figure 2: Countries with cyber security strategy (source: ENISA).[19]

portance of having credible institutions and policies. *Accountability is rarely in focus, and there is merit in assuming that there is not much point to speak about accountability of a non-existent or inefficient system.*

NUPI report on cyber security capacity building challenges this view by noting that access to cyberspace is growing faster than the institutions and frameworks that states use to support it.[20] This growth in access is positively received in the developing countries as it allows more people to connect to cyberspace and the Internet which in turn is seen as to boost the economy.[21] However, without institutional stability and legal frameworks, increased access can create more damage than benefits.[22]

The following sections will, using examples from Serbia, show how the experience from the SSR could actually help in building credible, effective and accountable cyber security institutions. We will argue that taking accountability, in contrast of considering only the effectiveness issues, as early in the process as possible, may significantly increase the chance for building effective institutions and policies.

In addition, if initiatives for establishing the cyber security institutions aim at overcoming challenges inherent for the SSR in general, they may contribute to SSR processes, many of which are already essential for wider institutions' capacity building (for example, chapters related to SSR in EU integration processes).

Potential for Connecting Cyber Security Institution Building and SSR – Examples from Serbia

First generation of SSR concerns the establishment of new institutions, structures and chains of responsibility for the security sector. Second generation SSR concerns the consolidation of previous reforms, and the effective and efficient operation of institutions, and procedures at a sustainable cost for the state and society.[23]

Based on the information presented in the EU accession progress reports on Serbia,[24] it may be concluded that Serbia now implements second generation of SSR, as defined by Edmunds.[25] The predominant context for the security sector, as well as other strategic development reforms in the country, are deeply anchored in the EU membership negotiations process.

Clearly, the EU has not considered cyber security as a component of SSR. But the connections are inevitable and most visible in the area of fighting against cyber crime.

The 2014 EU progress report for Serbia notes two issues related to cyber security and SSR:[26]

- Cyber crime: the High-Tech Crime Unit is still understaffed and needs to strengthen its capabilities. Partnerships with the public and private sectors and academia remain to be concluded. Further specialised training, better coordination between institutions, and adequate budgetary resources are needed.
- Protection of personal data: video surveillance, biometrics, the security of data on the internet, and the processing and protection of sensitive data must comply with EU data protection legislation.

It is noteworthy that the observation related to cyber crime discusses effectiveness, while the observation on protection on personal data reflects one of the core issues related to accountability. Two key principles of SSR are thereby discussed in the EU progress report. This illustrates two important points. First, that the EU has already well integrated principles of SSR into its monitoring methodologies (and, subsequently, the provision of assistance). And second, the link between cyber security and SSR, although not explicitly mentioned, clearly exists in EU's approach to assessing and supporting developments in Serbia.

Fortunately for Serbia, the institutions responsible for providing cyber security are not included as part of the security sector by the EU. If they were, it would have to be noted that that part of the security sector is still overwhelmed by the first generation of reforms, as defined by Edmunds.[27]

A crucial piece of legislation that should regulate the set-up of cyber security institutions in Serbia is the Law on Information Security. Previous Serbian governments have made several attempts to pass the Law but it has never reached the Parliament. The Serbian Government appointed in spring 2014 has made another attempt to submit a draft to the parliament. A working group was formed and prepared a draft in 2015, later on a series of public consultations were held. The ministry in charge of preparing the draft and sending it to the parliament—Ministry of Trade, Tourism and Telecommunications—had announced that the Law will be passed during the autumn of 2015.[28] The Law was actually passed in January 2016, in the dawn of new early elections in Serbia that took place in spring 2016.

At the moment this paper was written, cyber crime related issues in Serbia are regulated by the Criminal Code (in line with Budapest Convention on Cyber Crime [29] and the EU directive on attacks against information systems [30]). The police and the judiciary have functioning units specialised in such field.

However, Serbia is still among the countries without a functional national CSIRT (Cyber Security Incident Response Team), without national cyber security strategy and policy.[31] There are capabilities in various governmental agencies, dealing with some aspects of cyber security (security-intelligence services, the Ministry of Defence and the armed forces, specialised units of the government, academic and private institutions). *Yet, these capabilities are not efficiently coordinated on the national level, nor are there documents defining national policies related to security in cyberspace* (the National Strategy for the Information Society Development in the Republic of Serbia until 2020 [32] identifies information security as one of the priorities, but does not prescribe implementation deadlines or modalities; the National Security Strategy,[33] adopted in 2009, refers to threats from cyberspace, but only in a descriptive manner).

The national CSIRT is a crucial element of the national cyber security system. ENISA describes CSIRT's task as to respond to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution. In order to mitigate risks and minimize the number of required responses, most CSIRTs also provide preventive and educational services for their constituency. They also issue advice on vulnerabilities and viruses in the soft- and hardware running on their constituent's systems.

Hence, the national CSIRT should serve as a national platform for coordination and exchange of not only responses, but also proactive measures, i.e. policies.

The security sector institution in Serbia that stands the closest to a CSIRT is the Office of the National Security Council and Classified Information Protection.[34] It is, like the CSIRT, a technical body of the government, tasked to facilitate and coordi-

nate the information exchange among various agencies, and to protect classified data, thus providing administrative and technical assistance to the National Security Council and Coordination Bureau's activities.[35] The Office was established in 2009, as part of the governmental efforts to better use and to enhance the capacities dispersed among various governmental agencies (much like CSIRT will be). Additionally, it was given a central role in the implementation of a systemic law, to be observed by a wide number of governmental and private entities (in the case of the Office, this is the Law on Classified Information, while in case of a CSIRT it would be the Law on Information Security, according to the current draft).

According to Gajin and Matic,[36] two sets of problems have prevented the Office from effectively implementing the authority given by the Law on Classified Information during the five years since its adoption:

- First, the regulatory framework has been incomplete – even five years after the adoption of the Law. Sub-laws and complementary laws (most notably the Law on Information Security) were not passed;
- Second, there has been an array of problems diverging from the practice of Serbian public administration work – insufficient human resources for implementation of the law, absence of wide and permanent education, lack of awareness, and unpreparedness of some authorities for the implementation of the Law, etc.

The recently adopted Law on Information Security also envisages a set of sub-laws and regulations, directives, guidelines and similar acts, which should enable its full implementation. As mentioned above, there are dispersed capabilities in different institutions. Efficient distribution of responsibilities and authorities, as well as the reorganisation of these functions will require significant effort, and may cause certain resistance to change.

In addition, awareness about cyber security and threats from cyberspace is low in Serbia. Evident absences of wider public pressure for more government action in the area of cyber security as well as the absence of cyber security-related content from educational curricula on all levels testify in support of this claim. Neither citizens nor institutions can benefit from sustainable, permanent (even short-term) awareness-raising campaigns or adequate curricula in education institutions.

Although big companies are most often initiators and sponsors of awareness raising campaigns for citizens, there are no such campaigns for small and medium enterprises (SMEs). Government implements legality of software controls, but offers no advice or support for protection of SMEs from cyber threats.

Although the role of the private sector is of a crucial importance for cyber security, and vice-versa, most notably due to the fact that it owns a significant portion of information infrastructure. There is no structured communication platform between the government and the private sector not only for incident reporting, but also for consultations among private and public sectors in policy-making.

A particular problem is in fact that government employees are not sufficiently aware of cyber security challenges, while they directly affect the creation and implementation of government policies. However, there is no evidence of structured government-wide coordination of available human and technical resources for cyber security, even information exchange among different governmental departments and agencies on cyber security issues. In December 2014, the SHARE foundation,[37] a non-governmental organisation from Serbia, informed that a government agency had put on the internet approximately 1,22GB of personal data of over 5 million citizens. SHARE first informed the authorities, made sure the data was no longer on-line, and then published the alarming facts.

The adoption of the Law on Information Security will be a crucial point for cyber security institution building in Serbia, as it will be the first national formal act attempting to holistically regulate this area. A national CSIRT should play a crucial role in its implementation, and there are evident parallels and experiences that can be drawn from the challenges faced by the Office of the National Security Council and Classified Information Protection. Drawing from that, it is important to ensure that the drafting and adoption of necessary sub-laws and other necessary documents is done as soon as possible. In parallel, it is crucial to ensure adequate capacities are developed with the CSIRT and its role is recognised by all relevant stakeholders.

In addition, we will describe three initiatives, implemented in 2015 in Serbia, that demonstrate that a significant impulse for the building of cyber security institutions may come from activities and actors related to SSR processes.

The examples presented bellow illustrate the importance and benefits of the holistic approach to cyber security institutions building, in line with the core principles of security sector reform.

Example no.1: "Towards a National Cybersecurity Framework in Serbia: Building a Multi-stakeholder Platform"

The OSCE Mission to Serbia sponsored a project "Towards a National Cybersecurity Framework in Serbia: Building a Multi-stakeholder Platform,"[38] which was implemented by Diplo Centar (Serbian branch of the Diplo Foundation [39]). The local office of the Geneva Centre for Democratic Control (DCAF) [40] also supported the project's implementation. The main goal of the programme was to support the multi-

stakeholder process of developing institutional mechanisms in Serbia for addressing the risks emerging from cyberspace.

In a series of activities from March to June 2015, the project aimed and succeeded at gathering all relevant national stakeholders from the public and private sectors and facilitating a debate that should support the advancement of the national cyber security framework.[41]

What was unique about this endeavour was that it has achieved to, for the first time, gather into one forum relevant representatives of all security sector institutions (police, military, and intelligence), governmental institutions, agencies in charge of information society (telecommunications, privacy protection, etc.), private sector (telecoms, internet service providers, banks, major ICT companies), academia and non-governmental organisations. As testified by participants in the project, this was the first time they have met the majority of participants (even if both were working for different departments of the government).

This would not have been possible if three organisations, aware of the importance of the multi-stakeholder approach, did not join forces in identifying relevant organisations and ensuring their participation. Diplo Foundation invested its reputation and experience from activities in the area of internet governance, while OSCE and DCAF used their experience and good reputation from supporting SSR processes in Serbia for over a decade. Each partner was, in a way, an assurance factor to all invited institutions that the project will lead to a meaningful reform effort.

Apart from the publication, a major output of the project has been the establishment of a network of professionals (maintained by DIPLO's online platform, and which can be expanded) which offers a solid base for competent debate about the future set-up of the national cyber security institutions. The fact that the network fosters direct, informal relations among officials of various governmental departments also improves the horizontal communication among these institutions, a problem that has been recognised long ago in the SSR endeavours. In other words, the existence of this network may also indirectly support more efficient SSR.

The network already managed to provide constructive comments to the draft Law on Information Security. Its members also actively participated in the OSCE Chairmanship Event on Effective Strategies to Cyber/ICT Security Threats, held in Belgrade on 29 and 30 October 2015.[42] The OSCE Mission to Serbia also used this network to support the development of the starting points for national strategic documents on cyber security in November 2015. This was done through simultaneously increasing network members' capacity through exchange with international experts, and work on formulation of inputs that can be used by institutions given the mandate to develop such strategic documents in the near future.

By practicing a holistic approach to reforms, three organisations managed to provide a momentum that may underpin future cyber security institution building and SSR in Serbia.

Example no.2: Building Cyber Security Capacity in Serbia's Ministry of Interior

Reforms at the Serbian Ministry of Interior and the police service address one of the first reform areas where international community started investing a lot of efforts and funds after the democratic changes in 2001. However, these efforts did not match neither donors' nor beneficiaries' expectations in terms of efficiency, strategic alignment and, consequently, sustainability of reform efforts.[43] This was partly due to the fact that the ministry employs over 45,000 persons nation-wide, and is one of the most complex parts of the government apparatus both in terms of size and tasks. But insufficient alignments of reform efforts on both donor and beneficiary side certainly have contributed to this.

In 2015, the ministry announced that it will, in line with its ICT development strategy and action plan, revisit and upgrade its cyber security policies and functions. Concretely, formation of a unit designated to information security (Information Security Department, or ISD), and ministry's cyber security incidents response team ("MUP CSIRT").[44]

This is a very important development, also linked to the EU integration processes. Namely, Serbian Government's Action Plan for the chapter 24 of EU membership negotiations (AP 24) calls for the development of a safe platform for communicating between law enforcement bodies, that will provide more efficient coordination and collaboration of all the authorities responsible for the effective operation in the fight against organized and other forms of crime. This requires the adjustments to the normative framework and development of ICT infrastructure that ensures a high degree of availability and security. To achieve this, it is necessary to plan and implement extra resources for the purpose of reaching the appropriate standards applicable to the management of critical information infrastructures in the EU.

Having in mind that the ministry's ICT development strategy is supported by a project funded by Sweden,[45] and that the donor community normally supports the priorities expressed through the government's strategic documents, such as the AP 24, it can be realistically expected that donor support for capacity building of ISD and MUP CSIRT will be provided.

Experience from the security sector reform processes in Serbia so far can lead us to forming several valuable recommendations that would significantly increase the effectiveness of these capacity building efforts. Recognising this, the Ministry has requested and received the assistance of DCAF—as an organisation specialised in se-

curity sector reform—to produce holistic and sustainable capacity building program for these bodies.

The proposed program encapsulates and supports the most significant reforms processes in the ministry – most notably, the reform of the human resource management system (HRM), an area in which DCAF already supported the ministry.[46] This approach is beneficial both for the HRM reform, as it provides example of efficient use of new procedures and structures, as it is for the cyber security capacity building: it sets preconditions for adequate staff selection and retention for new units.

Moreover, DCAF's multi-stakeholder approach to SSR offers a good basis for developing (and implementing, if it comes to that) reform initiative that will foster good cross departmental and cross sectoral (public-private-civil) communications. Last but not least, by teaming up with an organisation whose mission is to promote democratic governance and accountability in the security sector, the ministry demonstrates its readiness to ensure a transparent and accountable capacity building process.

Creating synergies with SSR processes and actors promoting accountability can positively influence the efficiency of capacity building efforts for the institutions in charge of cyber security.

Example no.3: Public Hearing on Cyber Security in the Serbian Parliament

On 10 September 2015, Serbian Parliament's Defence and Internal Affairs Committee (DIAC), with DCAF's support, organised a public hearing dedicated to cyber security in Serbia.[47]

Holding a public hearing is a form of DIAC's oversight activity, open to all interested MPs and the public. It is not often used by the parliament, particularly by committees in charge of security related issues. In line with its mandate, DCAF supported this activity of DIAC through provision of expert advice and speakers for the purpose of promoting transparency and good governance of the security sector.

The objective of this hearing was to inform the participants on the specifics of the cyber security threats in Serbia and the significance of cyber security for the overall security in the country, to deliberate on the Government's policies and efforts to ensure cyber security for the economy and the citizens, as well as consider the National Assembly's potential role in the development of policies in the field.[30]

The Parliament invited representatives of relevant ministries to attend and testify, alongside national and international experts. Representatives of relevant NGOs and academic institutions, alongside private sector, were invited as well, and the event was publicly broadcast on Parliament's website. The event gathered close to 100 par-

ticipants in the Parliament's building, and drew significant attention on social networks.

DIAC Chairwoman, Ms Marija Obradovic, MP, stated that the event was marked by the same keywords, same conclusions and same messages, that there have been no discordant notes no matter what country or sector the speakers came from. She invited participants to continue communicating with MPs and to support them in efforts to be actively engaged in the building of cyber security system in Serbia through their legislative and oversight activities.

The Parliament helped put cyber security in public focus and offered support to its efficient development. At the same time, DIAC was exercising the use of an oversight tool that can gather most diverse groups and increase transparency and accountability of security sector institutions.

Although the impulse for the organisation of the hearing came from DIAC's Chairwoman, Ms. Marija Obradovic, the complexity of the topic, as well as the wide range of interlocutors for such an event, makes it not too likely that the parliament would have organised the event without external support (DCAF in this case). Several months of preparations for this event clearly demonstrate that the longer-term planning on parliament's side need to be coupled with longer-term external support for such event to be successfully organised and achieve its results.

Nonetheless, the very fact that the parliamentary hearing on cyber security took place, and that it drew the public and political attention it did, is a strong impulse for encouraging national governmental and civil society actors engaged in both institution building and raising awareness in Serbian society. DIAC has positioned itself as a relevant national forum for future discussion on this topic, and may draw from the contacts and expertise obtained at the event when discussing security policies and legislation in its domain. It has also set the example of efficient usage of public hearings as proactive tool of the parliament to other committees. Last but not least, MPs and parliamentary staffers that have increased their understanding of the topic may more efficiently follow relevant national and international developments and debates.

Again, a synergy between SSR and cyber security institution building was achieved, benefiting both processes.

Conclusion

The concept of security has evolved and now encompasses a much wider array of actors than traditionally sought. In parallel, it has been observed through various dimensions, leading to the understanding that the principles of effectiveness and accountability must both be observed in order to consider a security sector as democrat-

ically governed. This is equally valid for the newest dimension of security – security in cyberspace.

Drawing from the understanding that the SSR represents a practically and internationally recognised method of achieving good/democratic governance of the security sector, we have highlighted several features of the SSR that correspond to the challenges that the processes of cyber security institutions building and policy making are facing, including:

1. Necessity of holistic approach that acknowledges various actors on security service provision, as well as beneficiaries (i.e. the multi-stakeholder approach);
2. Requirement of a wide range of skills and specific, not widely accessible knowledge;
3. Need for secrecy, as opposed to accountability and privacy;
4. Scarce resources for reform projects that will not grow;
5. Evident need for increased effectiveness and accountability.

The examples from Serbia's experience in 2015 demonstrate that practicing a holistic approach to cyber security institution building, by creating synergies with SSR processes and actors promoting accountability, one can the multiply positive effects for both processes.

The parallel drawn with the challenges the Serbian Office of the National Security Council and Classified Information Protection has been facing since its establishment demonstrates that the set-up of new cyber security institutions, whose task would be to coordinate various stakeholders and national processes (a national CSIRT or a similar body), need to pay attention to two sets of potential problems:

1. Problems deriving from incomplete regulatory framework – to avoid this, legislation should be as complete and comprehensive as possible from the onset, or the process of producing necessary lower-level legislation needs to be launched as soon as feasible;
2. Problems diverging from the practice of public administration work – insufficient human resources for implementation of respective laws, absence of wide and permanent education/lack of awareness, unpreparedness of some authorities for the implementation of the Law and similar. These challenges should be mitigated by the application of appropriate policies that, in the long run, can be only beneficial to the overall governance reforms.

The examples of initiatives implemented in Serbia during 2015, presented in this article, illustrate the importance and benefits of the holistic approach to cyber security institutions building in line with the core principles of SSR.

The OSCE Mission to Serbia-sponsored project "Towards a National Cybersecurity Framework in Serbia: Building a Multi-stakeholder Platform" demonstrates the importance of synergies and holistic, multi-stakeholder approach, for effective building of functional cross-sectoral networks that can contribute towards building the national cyber security capacity.

The cyber security capacity building initiative of the Serbian Ministry of Interior speaks of how SSR processes and actors promoting accountability can positively influence the efficiency of cyber security capacity building efforts.

The third example, the first ever public hearing on cyber security in the Serbian Parliament, illustrates that the parliament can be an effective starting point for a national debate on cyber security and a very efficient awareness raising tool. However, in the given context, adequate external assistance is crucial.

All given examples are demonstrating the interlinkage and mutual reinforcements between SSR and cyber security institution building processes, thus providing an argument for their close coordination or even integration in contexts similar to that in Serbia.

Notes:

1 Stephen Goldsmith and William D. Eggers, *Governing by Network: The New Shape of the Public Sector* (Washington, D.C.: Brookings Institution Press, 2004).

2 Heiner Hänggi, "Making Sense of Security Governance," in *Challenges of Security Sector Governance*, ed. Heiner Hänggi and Theodor H. Winkler (Münster, Germany: Lit Verlag, 2003), 3-23.

3 *SSR in a nutshell: Manual for Introductory Training on Security Sector Reform* (Geneva: Geneva Centre for the Democratic Control of Armed Forces, The International Security Sector Advisory Team (ISSAT), 2012): 4, Figure 7, http://issat.dcaf.ch/content/download/2970/25352/file/ISSAT%20LEVEL%201%20TRAINING%20MANUAL%20-%20SSR%20IN%20A%20NUTSHELL%20-%205.3.pdf, accessed October 24, 2015.

4 *The United Nations SSR Perspective* (New York: United Nations, Department of Peacekeeping Operations, Office of Rule of Law and Security Institutions, Security Sector Reform Unit, 2012): 13, https://peacekeeping.un.org/sites/default/files/ssr_perspective_2012.pdf, accessed August 14, 2015.

5 Alan Bryden and Heiner Hänggi, eds., *Security Governance in Post-Conflict Peacebuilding* (Geneva: DCAF, 2005), https://www.dcaf.ch/sites/default/files/publications/documents/YB2005.pdf, accessed November 30, 2015.

[6] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar, What Everyone Needs to Know* (Oxford: Oxford University Press, 2014): 13.

[7] Europe Internet Stats: Serbia, http://www.internetworldstats.com/europa2.htm#rs, accessed August 14, 2015.

[8] OECD DAC handbook on security sector reform calls for holistic approach when devising reform policies. This is reflected in numerous other publications and development of organisations' policies.

[9] "List of official definitions as per different countries' documents," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Tallinn, Estonia, https://ccdcoe.org/cyber-definitions.html, accessed August 14, 2015.

[10] "UNDP Working Definitions," UNDP, November 2015, https://popp.undp.org/SitePages/POPPDefinitions.aspx.

[11] Heiner Hänggi, "Conceptualising Security Sector Reform and Reconstruction," in *Reform and Reconstruction of the Security Sector*, ed. Alan Bryden (Münster: LIT Verlag, 2004): 3, http://52.10.59.203/documents/85097/87432/Conceptualizing+Security+Sector+Reform+and+Reconstruction/9531f42c-0919-45d5-b51c-f6c2a090bb43?version=1.0.

[12] Benjamin S. Buckland, Fred Schreier, and Theodor H. Winkler, "Democratic Governance Challenges of Cyber Security," *DCAF Horizon 2015 Working Paper* no. 1, https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

[13] Buckland, Schreier, and Winkler, "Democratic Governance Challenges of Cyber Security."

[14] "Implementing SSR sector by sector," in *The OECD DAC Handbook on Security System Reform: Supporting Security and Justice*, Section 7 (Paris: OECD Publishing, 2007): 112-113, https://doi.org/10.1787/9789264027862-9-en.

[15] Hänggi, "Making Sense of Security Governance."

[16] Hänggi, "Making Sense of Security Governance."

[17] ENISA - European Union Agency for Network Information Security, www.enisa.europa.eu.

[18] National Cyber Security Strategies (NCSSs) Map, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map, accessed August 14, 2015.

[19] Map source, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world, accessed August 14, 2015.

[20] Lilly Pijnenburg Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities," Report no. 3 (Oslo: Norwegian Institute for International Affairs – NUPI, 2015).

[21] David Burt, Aaron Kleiner, Paul Nicholas, and Kevin Sullivan, *Cyberspace 2025: Navigating the Future of Cybersecurity Policy* (Microsoft Corporation, 2014), https://cloudblogs.microsoft.com/microsoftsecure/2014/06/02/cyberspace-2025-todays-decisions-tomorrows-terrain/, accessed April 7, 2015.

[22] "Africa 2013: Cybercrime, Hacking and Malware," *IDG Connect*, June 24, 2013, https://www.idgconnect.com/idgconnect/analysis-review/1009430/africa-2013-cyber-crime-hacking-malware, accessed June 18, 2016.

[23] Timothy Edmunds, "Security Sector Reform: Concepts and Implementation," in *Sourcebook on Security Sector Reform*, ed. Philipp Fluri and Miroslav Hadzic (Belgrade: Goragraf, Geneva Centre for the Democratic Control of Armed Forces, and Centre for Civil-Military Relations – Belgrade, 2004), 50.

[24] "European Neighbourhood Policy and Enlargement Negotiations – Serbia," European Commission, 2015, http://ec.europa.eu/enlargement/countries/detailed-country-information/serbia/index_en.htm, accessed 25 October 2015.

[25] Edmunds, "Security Sector Reform: Concepts and Implementation."

[26] European Commission, "Serbia: Progress Report," October 2014, http://ec.europa.eu/enlargement/pdf/key_documents/2014/20140108-serbia-progress-report_en.pdf, accessed October 25, 2015.

[27] Edmunds, "Security Sector Reform: Concepts and Implementation."

[28] "Ljajić: U oktobru zakon o informacionoj bezbednosti," *Blic* (in Serbian language), http://www.blic.rs/vesti/drustvo/ljajic-u-oktobru-zakon-o-informacionoj-bezbednosti/gf4n3p2, accessed September 23, 2015.

[29] Council of Europe, "Convention on Cybercrime," Full list, ETS no. 185, 2004, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, accessed October 25, 2015.

[30] "Directive 2013/40/EU of the European Parliament and of the Council," *Official journal of the European Union*, 14 August 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF, accessed October 25, 2015.

[31] Newly adopted Law on Information Security envisages the formation of national CSIRT with the national telecommunications regulatory body (RATEL); however, this body is not yet functional (August 2016). The Working Group for the development of national cyber security strategy has been established by the government following the adoption of the Law, but the results of their work (first draft strategic documents) are expected later in 2016.

[32] "Strategy for Development of the Information Society in the Republic of Serbia till 2020," *The Official Gazette of Republic of Serbia*, no. 55/05, 71/05-correction, 101/07 and 65/08, (in Serbian language).

[33] *National Security Strategy of the Republic of Serbia*, October 2009 (in Serbian language), http://www.kombeg.org.rs/Slike/CeBezbednost/statika/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf.

[34] Republic of Serbia, Office of the National Security Council and Classified Information Protection, http://www.nsa.gov.rs/eng/index.php.

[35] NSA Serbia, Support to the National Security Council and the Coordination Bureau for Security Services, http://www.nsa.gov.rs/eng/savet-i-biro.php.

[36] Sasa Gajin and Goran Matic, eds., *Primena zakona o tajnosti podataka* (OSCE Mission to Serbia, 2014).

[37] SHARE Foundation, https://www.sharefoundation.info/sr/.

[38] OSCE Mission to Serbia, http://www.osce.org/serbia.

[39] Diplo Foundation, http://www.diplomacy.edu/.

[40] Geneva Centre for the Democratic Control of Armed Forces (DCAF), http://www.dcaf.ch/.

[41] A publication presenting project results is available at http://issuu.com/diplo/docs/ka_nacionalnom_okviru_za_sajber-bez, accessed October 25, 2015, Information about the final event is available at http://www.osce.org/serbia/165066.

[42] "OSCE Chairmanship Event on Effective Strategies to Cyber/ICT Security Threats," Belgrade, Serbia, https://www.osce.org/cio/194421, accessed October 29, 2015.

[43] Amadeo Watkins with Svetlana Đurđević-Lukić, Nemanja Milošević, and Jelena Radoman, "Security Sector Reform and Donor Assistance in Serbia 2000-2010," (Initiative for Peacebuilding, 2010).

[44] Announced by Assistant Minister Nedeljkovic, Head of Ministry's ICT Sector at the Public Hearing on Cyber Security in Serbian Parliament held on 10 September 2010, http://www.parlament.gov.rs/Odr%C5%BEano_javno_slu%C5%A1anje_o_sajber_bezbednosti_u_Republici_Srbiji.26780.941.html, accessed: 25 October 2015.

[45] "Support to the Strategic Development of the IT system within the Serbian Ministry of the Interior," The International Management Group – IMG, 2011, http://www.img-int.org/Central/Public08/Projects.aspx?by=Donor, accessed October 25, 2015.

[46] "Introduction of a Modern Human Resources Management," Concept to the Ministry of Interior of the Republic of Serbia (Republic of Serbia: Ministry of Interior, 2014), http://www.dcaf.ch/Region/Southeast-Europe/Projects/Serbia-Introduction-of-a-Modern-Human-Resources-Management-Concept-to-the-Ministry-of-Interior-of-the-Republic-of-Serbia, accessed: 25 October 2015.

[47] National Assembly of the Republic of Serbia, "Public Hearing on Cyber Security in the Republic of Serbia," http://www.parlament.gov.rs/Public_Hearing_on_Cyber_Security_in_the_Republic_of_Serbia.26781.537.html, accessed October 25, 2015.

About the Author

Milan Sekuloski has over 10 years of experience in project management, governance, research and advisory in the area of security sector reform, mainly in Serbia. He holds a Master's Degree in Political Science, coupled with a university degree from the Military Academy of Serbia and Montenegro, and a number of non-degree courses in various areas. He has gained a holistic understanding of the reforms in the security sector area, as he has worked within the Armed Forces, Parliament and with national and international governmental and non-governmental stakeholders (OSCE Mission to Serbia, International Security Information Service Europe-Brussels, and the Geneva Centre for Democratic Control of Armed Forces, DCAF). Mr. Sekuloski has been actively involved in activities related to cyber security institution building in Serbia.