GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

MARCH 2018 No. 1

STRATEGIC SECURITY ANALYSIS

The Increasing Importance of Hybrid Politics in Europe:

Cyber Power Is Changing the Nature of Politics

by Aapo Cederberg and Jarno Limnéll

1 Introduction

Europe is becoming increasingly digital – and the development of digitalisation and emerging technologies is accelerating. Cyberspace has become an indispensable area of human activity, a sphere of regular security breaches and data threats, and an arena for inter-state conflict. When considering cyberspace from the nation state's point of view, we must keep two intensifying trends in mind. Firstly, today's cyber-related questions have become highly politicised. Thus, political commitment to and guidance on the development of cyberspace need to be strengthened. Secondly, cyberspace has created a new domain of warfare and is influencing the so-called cyber dimension of modern hybrid warfare. Hybrid threats have become one of the most prominent security challenges and an important part of security cooperation in Europe.

This paper examines the concepts of cyber politics and cyber-enabled hybrid warfare. It pays specific attention to the vulnerabilities of modern Western societies from a strategic-political perspective. The paper concludes that instead of cyber politics as such, a new kind of politics is needed – hybrid politics. Hybrid politics will be presented as a potentially winning concept for European security.

2 What is cyber politics?

In recent years issues related to cyberspace and its uses have risen to the highest levels of international politics, creating an area and discipline known as cyber politics. Cyberspace used to be considered largely a matter of low politics, and background conditions and processes. Today, cybersecurity is a focal point of conflicting domestic and international interests – and a rapidly developing factor in the projection of state power.

It is becoming increasingly important to understand cyberspace as a political domain. Politically, this is often neglected or forgotten. When considering cyberspace from the nation state's point of view, topical cyber-related questions have become highly politicised. The cyber domain should therefore primarily be treated as a political domain. When politics is involved, questions of power are always present. For example, in the context of war, cyber instruments are – like land, sea and air power – the means to achieve a political aim or increase a nation

KEY POINTS

- Issues related to cyberspace and its uses have risen to the highest levels of international politics, creating an area and discipline known as cyber politics.
- Protecting critical infrastructure and services from cyber threats is a complicated matter.
- The cyber domain is a central part of modern hybrid warfare, and malicious cyber-technical and cyber-psychological threats have both increased.
- Hybrid politics is a useful concept to describe both the importance of a holistic approach and the nature of high politics in the modern security reality.
- Hybrid politics is constantly changing the modern political process.
- The European Union (EU) should primarily understand hybrid politics as a potentially "winning concept" and take active steps to implement and sustain this understanding.

state's power.[1] The strategic use of cyberspace to pursue political goals and to seek geostrategic or authoritarian advantages is increasing. There is also a growing need for cyber norms and cyber diplomacy to be created through political processes.

With the creation of cyberspace and our deepening dependence on it, a new arena for the conduct of politics is taking shape. This process is described as "cyberization"[2], which refers to the ongoing penetration of all political fields by the various media of the cyber domain. The concept of cyber politics has therefore become useful, emphasising the importance of politics in cyber affairs. The term cyber politics refers to the conjunction of two processes or realities: (1) those pertaining to human interactions (politics) surrounding the determination of who gets what, when and how, and (2) those enabled by the uses of cyberspace as a new arena of contention with its own modalities and realities. As Choucri notes[3], all politics, whether in the cyber or physical arenas, involves conflict, negotiation and bargaining over the mechanisms, institutional or otherwise, to authoritatively resolve contentions over the precise nature of particular sets of core values.

Cyber politics is employed across the world – largely by academics interested in analysing the concept's breadth and scope and the use of cyberspace for political activity. It is applicable at both the national and international levels. Yet cyber politics and the cyber domain have created new conditions that do not have clear precedents, even if cyber issues are central to nation states' foreign and security policies. In the coming years we will see the true content and extent of cyber politics through the actual cases that arise. We may then start talking about and using the concept of politics – which cyber affairs are an integral part of – without the need to emphasise the concept of cyber politics. However, especially political-strategic understanding and commitment on cyber issues are strongly needed. Cyber politics needs to be developed in order to create a trustworthy digital environment, because the challenges in cyberspace are primarily political.

3 The cyber challenge facing modern societies

The functioning of the modern, strongly interconnected, global economy is based on unhindered access to information, energy, and financial flows. Unintentional or – in the worst case – intentional disruptions of these flows negatively affect the states subjected to them and the global order as whole. Moreover, because these flows are intertwined, disrupting one of them will have a damaging effect on the others, potentially leading to a cascading failure that could endanger the whole system that is dependent on these flows.

Protecting critical infrastructure and services from cyber threats is a complicated matter. Several questions need to be clarified before cyber threats can be tackled in an organised and efficient way. Among these questions are: Which parts of the cyber infrastructure should be prioritised as super-critical? What are the responsibilities of key actors – i.e. private companies and national governments – in the affected space? What are the operating areas and mandates of national and supranational entities such as civilian organisations, police, the military, and international regulating bodies?

The vulnerabilities of modern societies are the main targets of cyber attacks. In the cyber context, vulnerability is commonly defined as weakness related to information technology. The EU Agency for Network and Information Security (ENISA) defines vulnerability as "The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved".[4]

A modern society's security is based on the need to identify vulnerabilities and risks at all levels of the whole ecosystem, including people, processes, technology and data – and also governance, where

1 J.A. Lewis, "Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine", in K. Geers (ed.), Cyber War in Perspective: Russian Aggression against Ukraine, Tallinn, NATO CCD COE Publications, 2015, pp. 39-47.

2 J.-F. Kremer and B. Müller, Cyberspace and International Relations: Theory, Prospects and Challenges, London, Springer, 2012, pp. xi-xvii.

3 N. Choucri, "Cyberpolitics in International Relations", in. J. Krieger (ed.), Oxford Companion to Comparative Politics, New York, Oxford University Press, 2012, pp. 267-271.

4 ENISA, "Glossary 2017", <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary>.

the prerequisites for success or failure are originally laid down. Identifying the need for a common understanding of the existing threats, regulations, standards, risks, and complexities will be essential for securing critical infrastructure and services in the future. It is up to the national authorities to decide who is responsible for the security of such critical infrastructure and services. In terms of potential targets, the most cited example are the vulnerabilities inherent in our critical infrastructure that could be taken advantage of to create major disruptions that could adversely affect the whole of society.[5] Comprehensive situational awareness and understanding, as well as credible action plans and well-trained personnel, can prevent cyber attacks and defend critical infrastructure against such attacks.

The building of a more resilient society should not be viewed merely as an extra burden for already economically struggling Western societies; it is also a wonderful opportunity. Structures that allow a society to respond in an agile way to hybrid threats also support our understanding of and ability to cope with the complex underlying interrelations that make modern societies so fragile. These defensive structures will help to make our societies more functional if decision-making processes become more transparent and inclusive.

4 Cyber-enabled hybrid warfare

The famous Prussian military theorist Carl von Clausewitz stated in the 19th century that war is always a continuation of politics through military means, or simply the expression of politics by other means. The United States has interpreted this statement to mean that "politics and strategy are radically and fundamentally things apart. Strategy begins where politics end".[6] Based on these theories, one could say that hybrid warfare[7] is today's continuation of politics using hybrid capabilities. The fundamental question remains: What is/are hybrid war or hybrid operations? There is no internationally agreed definition of hybrid war, and our definition of this concept is based on recent incidents and publications. Because war is always widespread and encompasses all forms of warfare, hybrid warfare can be seen as the carrying out of warfare operations in all possible domains using all possible means.

The often-cited Russian "Gerasimov doctrine" describes modern warfare as joint operations utilising a mix of military and non-military means to achieve political goals, and taking full advantage of the intentionally blurred line between war and peace.[8] In the history of warfare we have seen similar activities described in a variety of terms, including, for example, non-linear operations, low-intensity conflict, full-spectrum conflict, political warfare, unconventional warfare, irregular warfare, asymmetric warfare, and unrestricted warfare. Nevertheless, it is important to keep in mind that the art of war is developing all the time and we often encounter new mutations or revisions of previously well-known doctrinal approaches.

Our security environment has dramatically changed in recent years. The current situation can be described as "the New Normal", in terms of which the changes in our security environment occur significantly faster due to the digitalised and interdependent world we live in, the future is more unpredictable, and hybrid operations are carried out all the time. Targets of hybrid operations can be found across the whole of society and particularly in the vulnerabilities of modern societies.

The citizens of Finland often enquire whether these developments will lead to a new war. The answer is: not to a conventional war, but to a hybrid war. We therefore need to determine what exactly hybrid war is and how to build credible hybrid defences. Cyber space is a key domain of hybrid warfare and hybrid threats, and one could even say that without modern cyber capabilities, the ability to influence hybrid threats and warfare would not be possible. Cyber power is indeed a global game changer, bringing new asymmetries to power politics.[9] All aspects of our lives and functions of our societies will be transformed by the all-pervasive and hyper-connected process of digitalisation that is continually being developed.

5 R.A. Clarke, Cyber War: The Next Threat to National Security and What to Do about It, New York, HarperCollins, 2010.

6 R. Pommerin (ed.), Clausewitz Goes Global: Carl von Clausewitz in the 21st Century, Berlin, Miles-Verlag, 2014, p. 342.

7 "Hybrid war/warfare" are controversial concepts. See M. Kofman, "Russian Hybrid Warfare and Other Dark Arts", War on the Rocks, 11 March 2016, <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/>.

8 General V. Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", Voyenno-Promyshlennyy Kurier (original in Russian), 26 February 2013, <http://vpk-news.ru/articles/14632>.

9 J.S. Nye, Cyber Power, Cambridge, MA, Harvard Kennedy School, May 2010.

From an operational perspective, hybrid operations can be described as a combination of two or more violent or non-violent state means or power-projection capabilities to achieve a desired political end state. These means include, but are not limited to, political and economic tools, information warfare, the use or threat of military force, cyber attacks, and engaging in special operations.

A successful hybrid operation needs strong political leadership and a clear mandate for the operation, combined with both the will and ability to dedicate a wide array of resources to the operation at short notice. Secondly, an effective and wide-ranging intelligence apparatus is needed to scan target countries and draw up a list of vulnerabilities. This list – the list of targets – would be based on the acquired knowledge of the key vulnerabilities and weaknesses that exist in the society of the target country. The third critical precondition that is often associated with a hybrid operation is the information campaign preceding the operation.[10]

These campaigns are aimed at raising support for the operation both internally and in the target country, which was seen in the case of the "polite green men" in Crimea.[11]

It has been argued that hybrid warfare is in essence a process of winning, or achieving the set goals, with little or no fighting. To build on this idea, we can say that in hybrid warfare it is nearly impossible to say when actual fighting or organised violence – war in its classic form – begins. One of the core characteristics of hybrid warfare is that it intentionally blurs the distinction between the neatly separated Western categories of war and peace, and civilian and military operations. This blurring is achieved by utilising a wide variety of means – both violent and non-violent, military and civilian – in a carefully planned way without unnecessarily breaching the threshold of conventional war, even if the level of escalation varies.

Many nations are currently attempting to ascertain how to build a hybrid defence. Because of the whole-of-society nature of hybrid threats, preparing for and addressing them require strong measures.

10 A. Rácz, Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist, FIIA Report, Helsinki, Finnish Institute of International Affairs, 2015.

11 K. Giles et al., The Russian Challenge, London, Chatham House, 2015, chap. 6.

The preparedness arrangements in Finland offer a living example of the comprehensive security approach. Society's vital functions are secured through collaboration among the authorities, the business community, civil society organisations and individual citizens. This model[12] has been a key element in attempts to improve preparedness at the government and societal levels. The Finnish security concept involves all stakeholders in society, because hybrid attacks do not respect any artificial boundaries between sectors, or separate ordinary citizens from government or business entities. This concept seems to be the future way to build resilience in an entire society, which will be the backbone of hybrid defence in the near future.

5 European cyber politics in response to hybrid threats

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks." – Jean-Claude Juncker, President of the European Commission

In recent years the EU and its member states have been increasingly exposed to hybrid and cyber threats that comprise hostile actions designed to destabilise a region or state. Countering such threats has therefore become a priority of European security. This means that cybersecurity and hybrid threats have risen to the level of European high politics. The increasing role of cyber politics, in the context of hybrid warfare, is stated in several recently published European strategies and official documents. Among others, the EU's new cybersecurity strategy emphasises cyber preparedness, which is central to both the Digital Single Market and the EU´s Security and Defence Union.[13] The EU´s Joint Framework on countering hybrid threats describes how cyber attacks could disrupt digital services across the EU and how perpetrators of hybrid threats could use such attacks.[14] Resilience is one of the pillars of the EU´s Global Strategy,[15] which highlights the role of hybrid

12 Security Committee, Secure Finland, information on comprehensive security in Finland, Docendo, Offset Oy, 2015.

13 European Commission, "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU", 13 September 2017, <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN>.

14 European Commission, "Joint Framework on Countering Hybrid Threats", 6 April 2016.

15 European Union Global Strategy, "Shared Vision, Common Action: A Stronger Europe", June 2016, <https://europa.eu/

and cyber threats in European security.

There has been a strong call for the EU to adapt and increase its capacities as a security provider and enhance its capacity to counter threats of a hybrid nature. This calls for greater human, technical, legal and institutional capacities. Cooperation with NATO has also been deepening and the joint declaration of 8 June 2016 has enhanced both organisations' abilities to counter hybrid threats, including by bolstering resilience, working together in analysis and intelligence sharing, and expanding coordination on cybersecurity.[16] The establishment of the EU Hybrid Fusion Cell and the European Centre of Excellence for Countering Hybrid Threats constitutes concrete steps forward in high politics.

6 Time to talk hybrid politics

As discussed in this paper, the following trends should be emphasised in Europe:

- Issues related to the cyber domain have entered the realm of high politics.

- Europe´s dependence on the cyber domain is increasing, and so do the possibilities of attacking digital societies and their people.

- The cyber domain is a central part of modern hybrid warfare, and malicious cyber-technical and cyber-psychological intentions have both increased.

- A holistic security approach is needed to prevent and deter constantly changing cyber and other hostilities.

We believe that in the coming years new cyber elements will appear in hybrid warfare that are designed to stay below the threshold of a formally declared war. The importance of the cyber domain will increase in hybrid warfare and the hybrid exerting of influence. Hybrid warfare increases "the fog of war" – as well as the "fog of security" – and cyber activities are well suited to this context. However, there are usually no "cyber-only" operations. In most cases, it is likely that other instruments will be deployed simultaneously to exert influence on the target. Cyber issues cannot therefore be separated from the overall security/warfare context. The cyber element is thus an inseparable part of hybrid warfare, but other important hybrid instruments should be taken into account when considering cyber activities. We wish to emphasise a holistic, political-strategic approach.

The current trend in societies, businesses and warfare is a drive towards so-called cyber-physical convergence. When analysing cyber activities, it is crucial to understand the increasing interaction between these two worlds and their intrinsic interconnections. We believe that one of the largest challenges facing cybersecurity in the coming years will be to understand and operate in the combined cyber-physical environment. As long as the physical and cyber domains are treated as separate entities, there is little hope of securing either of them.[17] The convergence of cyber and physical security has already occurred at the technical level. It is vital to increase our political-strategic understanding of the interconnected physical-cyber security environment in order to wage successful hybrid warfare.

Western societies too often concentrate on analysing cybersecurity only from the technological – or so-called cyber-technical – perspective. But we should also see cyberspace as an information space; that is, we should approach it from a psychological or cognitive perspective. For instance, in Russia´s military thinking it is strategically decisive and critically important to control the domestic populace and influence adversary states. These cyber-psychological means attempt to change people's behaviour or beliefs in favour of the Russian government's objectives.[18] We believe that the distinction between the cyber-technical and cyber-psychological domains will be more blurred and more combined in the coming years, and both aspects of the process of exerting influence through cyber-related means will have to be considered simultaneously.

It should also be noted how cyber operations and activities in warfare are increasingly becoming more integrated with other types of operations and activi-

globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web_0.pdf>.

16 NATO, "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization", 8 July 2016, <https://www.nato.int/cps/de/natohq/official_texts_133163.htm>.

17 J. Limnéll, "The Cyber Arms Race Is Accelerating – What Are the Consequences?, Journal of Cyber Policy, Vol. 1, 2016.

18 M. Connell and S. Vogler, "Russia´s Approach to Cyber Warfare", March 2017, <https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf>.

ties. For example, NATO not only sees the cyber domain as an additional domain of warfare, but is also increasingly integrating cyber capabilities into other military capabilities.[19] A comprehensive approach that connects capabilities in all warfare domains should be emphasised.

In today´s security environment, in vulnerable digital European societies and in the modern hybrid warfare era, cyber issues are achieving more importance in EU strategies, but often separately from other security-related areas. In politics especially, it is necessary to emphasise a holistic approach where cyber issues form part of all areas of politics. We see that "hybrid" as a concept is useful in thinking about security, since it embraces the interconnected nature of today´s threats and risks that we are experiencing. It also illustrates the multiplicity of actors and the diversity of the physical and digital means that are used both to initiate threats and defend against them. Therefore, in politics "hybrid politics" is a cogent term to describe both the importance of a holistic approach and the nature of high politics related to these matters. One challenge lies in the fact that current policy actions and responses are based on a rather static and siloed picture of the security environment, while not recognising the dynamic and holistic nature of hybridity.[20] The implementation of a holistic approach in politics will enable the EU, in coordination with its member states, to counter threats of a hybrid nature by creating synergies among all the relevant instruments and fostering close cooperation among all the relevant actors.

In the hybrid warfare toolbox, cyber operations are not just one capability – they create interdependencies among all the potential domains of hybrid operations. Cyber operations also play a critical role in information operations, economic sanctions and exerting influence on a target, as well as in military operations. The possibility of using cyber activities and influencing information expresses in many ways hybrid politics' potential for aggression. Hybrid politics has also had an impact on the use of military power in frightening ordinary citizen and boosting the media impact of specific actions.

19 NATO, press conference, 8 November 2017, <https://www.nato.int/cps/en/natohq/opinions_148417.htm>.

20 I.e. processes through which certain situations evolve to become hybrid threats or result in the hybrid exerting of influence and the motivations or reasons behind these processes (European Parliament, Countering Hybrid Threats: EU-NATO Cooperation, March 2017, <http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf>).

7 The cycle of hybrid politics

In politics, some factors change over time, while others will most probably not. One of the latter type is human nature. The element of power is always present in politics and warfare. Even if the nature of the security environment changes, human nature will essentially pursue its own interests, which, in the absence of control by a higher power, will likely lead to conflict. Yet, warfare and ways of pursuing power change over time – as does politics. Politics therefore has to change as its context changes. Continuous change is crucial particularly in hybrid politics in order to successfully prevent and deter various hybrid threats.[21] In this context, politic-strategic analysis and political commitment will be increasingly needed in the coming years.

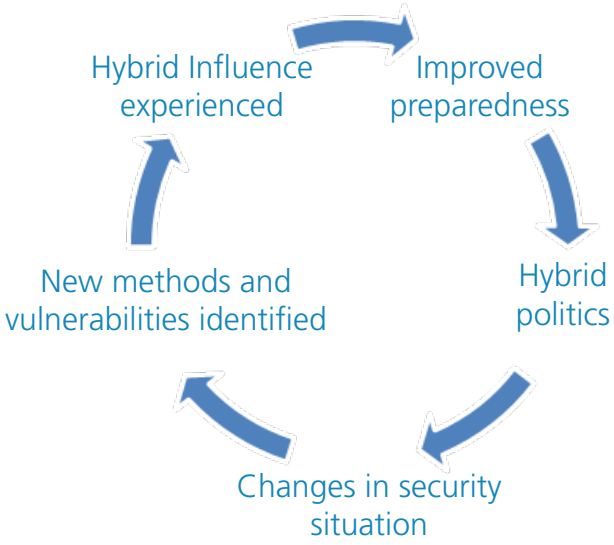

Figure 1. The cycle of hybrid politics

Both as a concept and as a practical tool, hybrid politics must be understood as a cycle, which is depicted in Figure 1.

Hybrid politics is constantly changing the ways we do politics. The objective is always to improve security. As described earlier in this paper, a comprehensive approach to using hybrid methods to exert influence is essential. Both political and practical improvements can be implemented either on

21 A good example is attempting to influence Western countries' elections (as part of exerting hybrid influence), which lie at the heart of democracy.

a reactive or proactive basis, both of which aim to improve preparedness. However, new ways of exerting hybrid influence over human nature will arise in which the significance of the cyber domain and the constantly developing technological methods of exerting influence are emphasised. It should also be noted that a hybrid campaign to exert influence may not be seen (and understood beforehand) until it is already well under way.

The exerting of hybrid influence is often targeted at critical functions that are vulnerable. Therefore, it is important in hybrid politics to regularly conduct a self-assessment of critical functions and vulnerabilities, both in reactive and proactive ways. It is also important to realise that not all vulnerabilities necessarily present themselves as opportunities for an opponent to exploit. The exerting of hybrid influence and improving one's understanding of vulnerabilities lead to changes in the security environment. In hybrid politics this means both taking action to respond politically to hybrid influence and the ability to improve security and preparedness.

The EU should primarily understand hybrid politics as a "winning concept" and take active steps to implement and sustain this understanding. The EU is seeking a new direction and content. European citizens expect to receive protection from the EU and want to feel secure in Europe. They also deserve it, because every European has the right to security. In the modern hybrid era, hybrid politics offers an opportunity both to respond to hybrid threats and to develop new models to deter aggression and design one's own best practices. One's own strategic analysis competence and effective intelligence-gathering capability lie at the centre of successful hybrid politics. The EU could also consider creating its own normative legal basis for cybersecurity and in this way increase the necessary cooperation among its member states.

8 Conclusion

Hybrid politics emphasises three key objectives that are vital to the EU and its future. Firstly, it focuses on a continuous understanding of ways of exerting hybrid influence and knowledge of one's own weaknesses. One should develop the appropriate abilities to fight back and develop one's resilience. This development requires a strong, ever-present political commitment and well-informed guidance. Secondly, hybrid politics should be an integral part of the EU´s deepening political and security policy cooperation. Responding to hybrid threats is a common interest shared by all EU member states, and hybrid defence should be based on a comprehensive security model applied throughout Europe. This cooperation would produce new "hybrid defence innovations" and best practices could be shared within the EU. Thirdly, it is important that the EU not only responds to any hybrid threats it experiences. The main objective of hybrid politics is to take the initiative back into the EU´s own hands in the modern, rapidly changing security environment.

About the authors

Mr. Aapo Cederberg´s current position is Executive Adviser to the Finnish Information Security Cluster (FISC) and Associate Fellow of the Global Fellowship Initiative at the Geneva Centre for Security Policy (GCSP). Aapo Cederberg is also CEO and Co-founder of Cyberwatch Finland. Cyberwatch is providing strategic analysis and better situational awareness of the cyber world for the management of companies and organizations in Finland.

Jarno Limnéll is Professor of Cybersecurity at Aalto University, Finland, and an adjunct professor in three other Finnish universities. Professor Limnéll holds a Doctor of Military Science degree in Strategy from the National Defense University in Finland; a Master of Social Science degree from Helsinki University and an Officer's degree from the National Defense University.

Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH-1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch