EGMONT POLICY BRIEF 295

– NOVEMBER 2022–

# Why Belgium Needs a Cyber Command

Alexander Mattelaer

***On 19 October 2022, the Belgian Ministry of Defence declared the Initial Operating Capability of its new Cyber Command. Responding to the trend of states seeking competitive advantages in a new operational domain – as illustrated by several high-profile cyber-attacks on Belgian State institutions – the choice for developing a new instrument of statecraft has been made. This Egmont Policy Brief outlines the growing importance of developing cyber defence capabilities, discusses the organisational set-up for this CYBER Command, and finally zooms in on the challenges ahead.***

Successive Belgian Defence reforms have attached increasing importance to cyberspace. The 2016 Strategic Vision document started to allocate dedicated financial resources to the development of cyber defence capabilities. The STAR-plan that the Council of Ministers agreed upon in June 2022 has amplified this emerging focus.[1] In the words of Minister of Defence Ludivine Dedonder, "Belgian Defence will significantly strengthen its cyber capability, which will eventually translate into the creation of a fully-fledged component."[2] These developments reflect an accelerating awareness that policy action is required to offset growing risks.[3] This policy priority is now trickling through every nook and cranny of the Belgian Defence establishment, most notably in the strengthening of defence research and technology efforts. The newly adopted Defence, Industry and Research Strategy, for instance, singled out the development of cross-domain cyber defence and "a robust civilian-military cyber ecosystem of excellence" as a priority.[4]

The setting-up of a dedicated Belgian Cyber Command (BECYBERCOM), not unlike the Special Operations Command created in 2018 and similar developments in other allied nations, constitutes a milestone in the fulfilment of this policy ambition. Not only does it reflect the organizational priority that the cyber domain receives, it also – and perhaps more importantly – provides the Belgian government and the defence staff with a truly operational instrument, that is to say, the capacity to act, protect and respond in today's threat environment. As the war against Ukraine has illustrated, the ability to harness fast-paced battle management data networks in real time is proving to be key to 21st century strategic competition, together with the acumen to exploit and instrumentalise the congested information space effectively. In essence, without adequate cyber capabilities, no effective joint effort combining air-, land- and naval power is possible anymore.

This Egmont Policy Brief offers a synthetic review of the rationale for setting up BECYBERCOM. The first section outlines the growing importance of developing cyber defence capabilities. This increase in importance stems from three distinct sources: the growing dependence on technology, the changing character of modern warfare, and the link with human cognition. The second section discusses the organisational set-up for BECYBERCOM. It highlights the hybrid nature of this functional command entity that cuts across the military intelligence service and the defence staff. Thirdly, it offers some thoughts on the challenges that the new command will face. In doing so, it pays special attention to matters relating to human resources, political oversight and civil-military relations more broadly defined.

EGMONT Royal Institute for International Relations

## WHY THE IMPORTANCE OF CYBER DEFENCE IS GROWING

The growing awareness about the need to boost cyber defences has been years in the making. Already a decade ago, news stories about cyberattacks against Belgian data networks began to proliferate.[5] During the spring of 2014, for instance, a cyber weapon known as Ouroboros infected not only dozens of Ukrainian computer networks, but also those of the Belgian Ministry of Foreign Affairs and many other European partners.[6] This pattern repeated itself in 2022, when Belgium together with all other EU member states attributed a new wave of cyberattacks to the Russian Federation.[7] In July 2022, the Belgian government went so far as to unilaterally attribute malicious cyber activities to Chinese hacking groups.[8] As this largely aligns with the trend of increasing cyberattacks on private companies and individual citizens, the pattern is clear: the cyber-threat against Belgian interests is real, growing, and intensifying.

Most fundamentally, the increasing threat level in cyberspace reflects a societal trend of ever-increasing dependence on ICT networks. The digitalisation of European economies constitutes an EU policy priority as well as a fact of life that has been greatly amplified by the Covid-19 pandemic. 'A Europe fit for the digital age' constitutes one of the six European Commission priorities for the legislative period 2019-2024. As digitalisation creates vulnerabilities too, this has been accompanied by major regulatory initiatives for cybersecurity, such as the Cyber Resilience Act and the NIS 2 Directive on measures for a high common level of cybersecurity across the Union.[9] It is therefore not surprising that individual member states develop and update national level cybersecurity strategies.[10] Similarly, this trend cannot leave defence establishments unaffected. In 2016 NATO recognised cyberspace as a domain of military operations, alongside the traditional domains of air, land, and sea.

This reflected the emerging realisation that cyberspace presents vulnerabilities, as well as opportunities, for defence establishments. In 2017 Belgium joined the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, the capital of Estonia that fell victim to a large scale cyberattack already in 2007. At the 2018 Brussels Summit, NATO allies agreed how to integrate sovereign cyber effects into Alliance operations and missions.[11] Similarly, the 2022 EU Strategic Compass heralded the development of an EU Cyber Defence Policy.[12]

What is perhaps not as widely understood, is how the cyber domain is changing the character of war itself. Not only are military forces growing more dependent on their communication and information systems, but modern warfare is itself increasingly concerned with the speed at which sensors, weapon systems and target sets can link up with one another in real-time, digital battle management networks. Pursuing military advantage thus necessitates a proverbial 'combat cloud' that relies on multi-domain command and control for realising kinetic effects – delivering munitions to target. In combination with the competitive, dyadic nature of war this implies that one's own digital footprint must be camouflaged and protected as well as possible, and that the neutralisation and disablement of the opposing network becomes an operational objective. In other words, the cyber domain does not only enable the fight, but it also increasingly becomes an integral component of the fight itself. While cyberattacks may sometimes offer an alternative to kinetic violence, successful cyber operations and effective combat clouds also increase the lethality of the force. The fact that the ICRC has just proposed the development of a digital red cross/crescent emblem speaks volumes in this regard.[13]

Finally, the cyber domain is increasing in importance because it interfaces directly with human cognition. Today, most information flows created by humans are embedded into digital media (rather than paper or other information carriers). On top of that, the digitalisation of information – and the corresponding decrease of the cost of information dissemination – has resulted in an exponential growth of the overall volume of information. This explosion of data concerns high quality and low-quality information alike, generating an information landscape that becomes increasingly difficult to navigate. Unsurprisingly, both state and non-state actors alike are

engaging in fierce information competition, seeking to influence perceptions and to shape the behaviour of citizens and adversaries alike. As the authority to arbitrate the quality of information becomes itself contested, the cyber domain morphs into an arena of increasingly sophisticated influence operations that challenge the human capacity to think freely and without prejudice. This is arguably an even more pressing concern for smaller states, as larger actors have an inherent advantage in terms of this narrative competition. In its most expansive definition, cyber defence comes to include not just the protection of critical ICT systems or the digital enabling of military operations, but ultimately the shielding of society against nefarious influencing writ large.

## WHAT WILL THE BELGIAN CYBER COMMAND LOOK LIKE

Against this background, the new Belgian Cyber Command will provide a single focal point guiding the development of cyberspace capabilities and directing all cyber operations. This section reviews the missions and tasks with which it has been endowed, the organisational set-up that has been designed, and the legal framework under which it operates.[14] Even though BECYBERCOM remains an organic part of the military intelligence service (ADIV/SGRS), its functional remit will stretch across the Belgian armed forces in their entirety. Finally, the inception of BECYBERCOM is also strongly anchored in an approach based on institutional partnerships with a wide variety of public authorities, the private sector, academic institutions, and civil society.

The set of missions BECYBERCOM is directed to accomplish is threefold. Within the electromagnetic and cyber space, it is responsible for (i) ensuring the intelligence and security missions of the military intelligence service, (ii) guaranteeing the freedom of manoeuvre of the Belgian armed forces, and (iii) generating military effects in support of defence operations. This translates into four tasks, namely (a) overseeing the readiness of the cyber resources of all Belgian Defence components (i.e. grooming the cyber readiness of all forces), (b) ensuring the readiness of the dedicated cyber forces, (c) maintaining readiness to implement specialised cyber defence capabilities in the context of aid to the nation and national crisis situations, and (d) conducting both defensive and offensive cyberspace operations as directed within the appropriate legal framework. In other words, BECYBERCOM not only protects critical ICT infrastructure and defends against attacks in cyberspace, but also collects intelligence through intrusive or non-intrusive operations and fights in cyberspace in support of (or in addition to) conventional military operations.

In organisational terms, BECYBERCOM was born out of the earlier Cyber Direction that existed within the military intelligence service ADIV/SGRS. The position of new Cyber Commander – a function first taken up by Major-General Michel Van Strythem as of October 2022 – is unique in the sense that it enables cyber operations to be executed under the command authority of the Chief of Defence as well as cyber intelligence operations under the direction of the military intelligence Chief. To that purpose, the Cyber Commander is assisted by a Deputy Commander (with subordinate teams responsible for defensive and offensive cyber operations, cyber collection and SIGINT, and digital influence collection) and a Chief of Staff that focuses on education, training, doctrine, innovation, and external relations. In the latter sense, the Cyber Command is akin to a defence component, i.e., centred around building and maintaining the readiness of the cyber forces.[15] Yet it also provides a focal point for nurturing unified command expertise in a way that resembles the existing Belgian Special Operations Command.[16]

The conduct of Belgian cyber operations can take place under two distinct legal frameworks. On the one hand, cyber operations can serve intelligence purposes. These corresponding operations fall under the remit of the 1998 law regulating the Belgian intelligence and security services.[17] This law has been recently amended so as to permit the military intelligence service to conduct offensive cyber operations in response to attacks on Belgian Defence ICT systems, or in case of a national cybersecurity crisis (in conformity with applicable international law.)[18] On the other hand, cyber operations that aim to generate military effects in support of Belgian Defence missions can

fall within the legal framework regulating the conduct of military operations. This includes the 1994 law on the use and readiness of the armed forces, the royal decree of 1994 concerning the commitment of the armed forces in peacetime, and the 1998 royal decree on the structure of the Ministry of Defence.[19] Under the latter framework, the constitutionally defined command authority of the King gets delegated to the Chief of Defence and then to the Assistant Chief of Staff for Operations and Training. This includes operational command authority over the cyber capabilities provided by the military intelligence service, alongside all regular units provided by the different service components. As such BECYBERCOM enables the merging of two distinct command hierarchies into a single focal point for all cyber operations.

Given the sheer novelty of the cyber domain that has emerged – and that is still relentlessly expanding – it comes as no surprise that BECYBERCOM is pursuing a wide range of partnerships. It cannot possibly hope to accomplish its different missions and tasks alone. These partnerships cut across the Belgian federal authorities and include the Centre for Cybersecurity Belgium, which resorts under Chancellery of the Prime Minister, the FPS Foreign Affairs, the National Security Authority, the Crisis Centre, and various cyber law enforcement authorities under the FPS Interior, and of course the public prosecutor, the Coordination Unit for Threat Analysis, and the civilian State Security agency under the aegis of the FPS Justice. Yet this partnership approach goes beyond the public sector. It also engages the private sector as well as academic institutions and civil society. Especially noteworthy in this regard is the role that is accorded to the Royal Military Academy as cyberspace knowledge hub operating in tandem with the civilian universities.[20] This goes hand in hand with the high priority the Royal Higher Institute for Defence gives to cyber defence related research through its various funding instruments.

## HOW TO WIELD A NEW INSTRUMENT OF STATECRAFT

With the Initial Operating Capability of the Cyber Command achieved, the Belgian government has a new sovereign instrument of statecraft at its disposal. It can now direct the Belgian Defence to accomplish politically defined objectives by means of cyber operations. This development enables the State to protect and further the security interests of Belgian society in new ways. Yet it also raises several new challenges. These relate to the management of expectations, which must inevitably be tailored to human resources available, the need for ensuring due oversight, and the way in which public authorities act and react in the realm of cyberspace-enabled influence operations.

The emergence of any new military capability cannot help but raise many questions in terms of what to expect. For some, new technologies can appear as cheap or quasi-magical solutions to all problems. For others, they can appear so daunting and complicated as to instil reticence and uncertainty. The challenge therefore will be to recruit and train enough cyber specialists to meet the high – if somewhat nebulous (because of the many questions) – expectations that have now been created. As in all other dimensions of defence capability development, Belgium has only embarked on the strengthening of its cyber defences when the hour was late. It will take many years to grow the personnel cadre, to upgrade the technical infrastructure, and to develop the required doctrine. All of these are needed to reach the capability level at which many allies and some adversaries already operate today. Full operational capability of BECYBERCOM is to be reached not earlier than 2030.[21] Policymakers must therefore remain acutely aware that adversaries may attempt – and potentially succeed – in overwhelming Belgian cyber defences while the long process of honing this new capability is underway.

A second important challenge concerns the framework for exercising civilian control and political oversight. The existence of two distinct legal frameworks and command hierarchies constitutes a double-edged sword. On the one hand, it enables the seamless transitioning from intelligence operations to military operations and back, hence consolidating all technical savvy into a single organisation. On the other hand, this set-up may initially confound lawmakers and government officials, for whom information gets compartmentalised into

different oversight frameworks. At heart, this challenge will require nurturing a cadre of experts at the political-strategic level (alongside the technical and operational levels, that is). The political level can only be expected to wield an instrument effectively to the extent that it is well-versed in its uses. The considerable attention that the Belgian Standing Intelligence Agencies Review Committee dedicates to cyber defence issues speaks volumes in this respect.[22] One of the most delicate issues for political arbitration concerns determining under what conditions a cyber-attack gets treated as an armed attack (or as a hostile act by a foreign power) rather than as a mere criminal act. This effectively determines when the response must switch from being governed by criminal law to the law of armed conflict, and potentially qualifies as a trigger for NATO's Article 5, TEU Article 42.7 or TFEU Article 222. In such cases, political arbitration will require synchronisation amongst allies and partners.

A third challenge concerns the approach taken towards cyber-enabled influence operations. While the Belgian Standing Intelligence Agencies Review Committee has observed that the military intelligence service has only few tools available for big data and datamining, digital influence collection will constitute an important domain of future investment. In combination with the activities of the Directorate-General for Strategic Communication within the defence staff, this will over time provide much greater awareness about hostile information and influence operations – and the means to counter them. BECYBERCOM is not tasked or mandated to become some sort of digital thought police, but it will become increasingly well-versed in deciphering the mind games that are being played by the manipulation of social media data and algorithms. While political parties have a well-defined interest in instrumentalising social media for electoral purposes, the defence and intelligence establishment will also continue to have a duty and responsibility to point out foreign interference in decision-making processes and in the constitutional order itself.

## CONCLUSION

The establishment of BECYBERCOM represents a milestone in the regeneration of the Belgian armed forces. Yet it does not constitute a panacea for confronting the growing problems in European and international security. The war that Russia has launched against Ukraine has provided a forceful reminder about the vital importance of nuclear and conventional deterrence.[23] Belgium still has a considerable way to go in terms of meeting its deterrence and defence commitments. Cyber defence will thus not substitute itself for other forms of military power, but it will continue to enable military operations and provide additional options for realising strategic effect. In that sense, BECYBERCOM is set to become a critical instrument of statecraft to be ready for the future, both within cyberspace and beyond.

At the same time, the strategic purpose of BECYBERCOM is not limited to Belgian Defence operations. As an intelligence instrument it serves a wider purpose that is deeply enmeshed in a political, economic, and social context. It offers the means to resist in the domain in which external aggression is likely to impact Belgian society the earliest in time – a pattern that may have already begun. Precisely because cyber threats may impact individuals, public institutions, and private companies in such an immediate way – in everyone's living room, so to speak – it is of critical importance to develop response instruments at the national level. This keeps in with the existing treaty commitments to pursue both self-help in national security and mutual aid towards allies. In that sense, BECYBERCOM is one of the few quintessentially sovereign capabilities at the service of the Belgian State and all its citizens.

***Prof Dr Alexander Mattelaer is a Senior Research Fellow at Egmont – the Royal Institute for International Relations. He is also an Associate Professor at the Vrije Universiteit Brussel, where he serves as Vice-Dean for Research at the Brussels School of Governance, and Chair of the Scientific Committee of the Royal Higher Institute for Defence.*** ***He is grateful to Sven Biscop, Pol De Witte, and several Belgian Defence officials for their comments on an earlier version of this text. The responsibility for any errors lies naturally with the author alone.***

# Endnotes

1 *STAR-plan: Security & Service, Technology, Ambition and Resilience*, approved by the Belgian Council of Ministers, 17 June 2022, https://dedonder.belgium.be/sites/default/files/articles/STAR%20Plan_NL.pdf .

2 *Policy Declaration of the Minister of Defence*. Brussels: Belgian Federal Parliament, 4 November 2020 (doc 55 1610/017), p. 25, https://www.dekamer.be/FLWB/PDF/55/1610/55K1610017.pdf .

3 For historical background, see Alexander Mattelaer, 'Een adaptieve krijgsmacht voor onzekere tijden', colloquium contribution to *De toekomst van Defensie*: Horizon 2030, 25 February 2015, pp. 84-91, https://www.egmontinstitute.be/app/uploads/2015/02/Papers_Wise_Pen.pdf .

4 Royal Higher Institute for Defence, *Defence, Industry and Research Strategy*, approved by the Belgian Council of Ministers on 16 September 2022, https://www.defence-institute.be/wp-content/uploads/2022/10/dirs-en.pdf .

5 See e.g. Kristof Clerix, 'Serious cyber attack hits Belgian military intelligence service', *MO Magazine*, August 2013, https://www.mo.be/en/article/serious-cyber-attack-hits-belgian-military-intelligence-service .

6 For discussion, see Alexander Mattelaer and Laura Vansina (eds.) *Dealing with Russia: Towards a Coherent Belgian Policy*, Brussels: Egmont Institute (Egmont Paper 109), p. 12, https://www.egmontinstitute.be/dealing-with-russia-towards-a-coherent-belgian-policy/ .

7 See the Belgium MFA retweeting the EU declaration on Russian cyber operations against Ukraine, 10 May 2022, https://twitter.com/BelgiumMFA/status/1524070462057234439?s=20&t=WfjX4dcr6mzMvwrMAdghWg

8 'Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors', 18 July 2022, https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities .

9 For info see https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act and https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985 , respectively.

10 In May 2021 the Centre for Cyber Security Belgium published its *Cybersecurity Strategy Belgium 2.0*, see https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_NL_DP6.pdf .

11 NATO Heads of State and Government, *Brussels Summit Declaration*, Brussels: NATO, 12 July 2018, § 20, https://www.nato.int/cps/en/natohq/official_texts_156624.htm .

12 *EU Strategic Compass for Security and Defence*, Brussels: Council of the EU, 21 March 2022, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf .

13 International Committee of the Red Cross, 'ICRC proposes digital red cross/crescent emblem to signal protection in cyberspace', 3 November 2022, https://www.icrc.org/en/document/icrc-proposes-digital-red-crosscrescent-emblem-signal-protection-cyberspace .

14 For more in-depth background, see Alexandre Daniel, 'La construction d'un Cyber Command', *Belgisch Militair Tijdschrift / Revue Militaire Belge* 24, 14 October 2022, https://www.defence-institute.be/wp-content/uploads/2022/10/rmb-24-art-01.pdf .

15 For an introduction to the concept of 'readiness', see Alexander Mattelaer, 'Readiness as a Mission: Implications for Belgian Defence', Brussels: Egmont Institute (Security Policy Brief N° 150), October 2021, https://www.egmontinstitute.be/app/uploads/2021/10/SPB150-Mattelaer-Readiness.pdf .

16 For reference, see Alexander Mattelaer, 'Why Belgium Needs a Special Operations Command', Brussels: Egmont Institute (Security Policy Brief N° 70), April 2016, https://www.egmontinstitute.be/app/uploads/2016/04/SPB70.pdf .

17 Wet houdende regeling van de inlichtingen- en veiligheidsdiensten, 30 November 1998, *Belgisch Staatsblad*, consolidated version available from http://www.ejustice.just.fgov.be/eli/wet/1998/11/30/1998007272/justel .

18 Ibidem, Article 11, §1, 2°.

19 Wet betreffende de perioden en de standen van de militairen van het reservekader alsook betreffende de aanwending en de paraatstelling van de Krijgsmacht, 20 May 1994, consolidated into http://www.ejustice.just.fgov.be/eli/wet/2007/02/28/2007007077/staatsblad ; Koninklijk Besluit houdende bepaling van de vormen van operationele inzet, hulpverlening en militaire bijstand, en van de voorbereidingsactiviteiten met het oog op de aanwending van de krijgsmacht, 6 July 1994, consolidated into http://www.ejustice.just.fgov.be/eli/besluit/1994/07/06/1994007183/justel ; Koninklijk besluit tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten, 2 December 2018, http://www.ejustice.just.fgov.be/eli/besluit/2018/12/02/2018015479/staatsblad .

20 This hub-model is centred around, among other things, the development of a cyber/cryptography/tempest lab focused on high-end certification and the development of mathematical research domains such as artificial intelligence for digital influence detection and quantum computing for cryptography.

21 Alexandre Daniel, op. cit.

22 Belgian Standing Intelligence Agencies Review Committee, *Activity Report 2021*, Brussels, 25 May 2022. https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2021.pdf .

23 Cf. Alexander Mattelaer, 'Rethinking Nuclear Deterrence: A European Perspective', Brussels: VUB Centre for Security, Diplomacy and Strategy (CSDS Policy Brief 13/2022), 23 May 2022, https://brussels-school.be/sites/default/files/CSDS%20Policy%20brief_2213.pdf .




www.egmontinstitute.be