KOMMERSKOLLEGIUM
NATIONAL BOARD OF TRADE SWEDEN

The Cyber Effect

The implications of IT security regulation on international trade

2018

The National Board of Trade is a Swedish government agency responsible for issues relating to foreign trade, the EU Internal Market and to trade policy. Our mission is to promote open and free trade with transparent rules. The basis for this task, given to us by the Government, is that a smoothly functioning international trade and a further liberalised trade policy are in the interest of Sweden. To this end we strive for an efficient Internal Market, a liberalised common trade policy in the EU and an open and strong multilateral trading system, especially within the World Trade Organization (WTO).

As the expert agency in trade and trade policy, the Board provides the Government with analyses and background material, related to ongoing international trade negotiations as well as more structural or long-term analyses of trade related issues. As part of our mission, we also publish material intended to increase awareness of the role of international trade in a well functioning economy and for economic development. Publications issued by the National Board of Trade only reflects the views of the Board.

The National Board of Trade also provides service to companies, for instance through our SOLVIT Centre which assists companies as well as people encountering trade barriers on the Internal Market. The Board also hosts The Swedish Trade Procedures Council, SWEPRO.

In addition, as an expert agency in trade policy issues, the National Board of Trade provides assistance to developing countries, through trade-related development cooperation. The Board also hosts Open Trade Gate Sweden, a one-stop information centre assisting exporters from developing countries with information on rules and requirements in Sweden and the EU.

www.kommers.se

National Board of Trade Sweden, June 2018 — First Edition. ISBN: 978-91-88201-38-6

Foreword

The importance of IT security is widely acknowledged. However, the increasing number of cyber incidents, attacks and breaches have made it evident that more robust policies and requirements need to be implemented. Governments need to protect individuals, businesses and society from the vulnerabilities accompanying the technologies we are using.

The regulation of IT security in Information and Communication Technology (ICT) products differs greatly from ordinary product regulation, which is mainly concerned with health, safety and the environment, since the objective of IT security regulation is also to secure critical infrastructure and national security. The approach taken by regulators, therefore, easily results in regulatory measures based on specific national conditions and requirements, rather than regulatory approaches that aim at global interconnectivity and international trade.

Are these regulatory measures with national deviations for IT security truly well grounded or are we seeing a rise in unnecessary protectionism?

Although increased governmental intervention may be necessary to improve IT security in society, very few of us have the competence to judge whether these regulations in fact are necessary, effective and take into account effects on all stakeholders or if these actions are the source of unnecessary barriers to international trade.

The consequences of an increasing number of diverging national regulatory strategies can become rather severe. A lack of transparency and consensus in IT security regulation for industrial goods not only risks market access for commercial ICT products and applications worldwide but also contributes to unfair competition, which may have an inhibitory effect on technological development. In other words, the stakes are high.

This report is written by Heidi Lund with advice from a number of colleagues at the National Board of Trade: Magnus Andersson, Linda Bodén, Sara Emanuelsson, Anders Karlsson, Anton Karlsson, Ola Landström, Henrik Isakson, Johanna Nyman, Magnus Rentzhog, Charlie Olofsson and Hiba Zeydi.

As the topic of this report falls partly outside the main working area of the National Board of Trade, contributions from external experts have been crucial. In particular, the National Board of Trade wishes to thank Dag Ströman, Managing Director of the Swedish Certification Body for IT Security (CSEC) located within Swedish Defence Materiel Administration (FMV); Helena Andersson, Strategic Advisor-Swedish Civil Contingencies Agency; Ronny Harpe, Strategist-Swedish Civil Contingencies Agency; and Staffan Persson, Managing Director of atsec for their valuable input during the process.

The National Board of Trade also wishes to thank the following persons and organisations (with members) for valuable comments: Curt-Peter Askolin, Lead Assessor- Swedish Board for Accreditation and Conformity Assessment (Swedac); Slawomir Gorniak, Expert- ENISA; Hans Hedbom, Lecturer- Karlstad University; Jan-Ove Larsson, Information Assurance Consultant (previously with National Defence Radio Institute); Mats Nilsson, Director of Strategy and Technology Practise - Ericsson, DIGITALEUROPE; and the Association of Swedish Engineering Industries members.

Stockholm, May 2018

Anna Stellinger
General Director
National Board of Trade

Executive Summary

IT security is one of the most important challenges of our time. However, countries use different strategies to address IT security depending on their national priorities.

The objective of this report is to describe the function of IT security, to define by which means IT security in Information and Communication Technology (ICT) products can be regulated and to highlight in which manner the regulation of IT security has a bearing on international trade and market access. The ambition of this report is also to discuss whether greater harmonisation of regulation in the field of IT security for ICT products is possible, as the current regulatory landscape is rather fragmented compared to many other product areas.

This analysis shows that the regulation of IT security in ICT products is a rather complex area, which does not follow the logic of product regulation in other domains. Further, the policy choices made in the domain of regulation will have a significant effect on our security and also on international trade.

While digitalisation makes our society increasingly effective, it has become evident that the technology we are using for communication and information sharing presents serious vulnerabilities. These vulnerabilities may manifest in cyber threats or incidents, unauthorised access to data, data loss or theft and denial of operations. These problems make IT security one of the most important questions of our time. When policy makers and regulators address IT security in ICT products, they should take note of a large number of interdependencies, including acknowledging that modern life is dependent on a multitude of interconnected and interdependent infrastructures so that separating cyberspace (as its own domain) from sectors such as food, health and transportation has become impossible. Cyberspace can be best understood as a thin layer running through all sectors, enabling them to communicate and function. In addition, our living and trading patterns are inherently based on global, rather than local, connections that need to be taken into account when addressing IT security in ICT products that are manufactured, distributed and installed worldwide. Environments at risk include, for example, businesses, smart cities, smart homes, energy systems, railway systems, air transport systems, smart grids and government bodies.

It is possible to address IT security in ICT products in several ways. One method concerns product regulation. The regulations that are prepared, adopted and applied for IT security for ICT products differ significantly from ordinary product regulation, as these regulations need to address societal infrastructure concerns, privacy concerns and national security issues as well as health, safety and environmental concerns. This difference arises because most ICT tools and

IT security regulation as a policy challenge

NATIONAL SECURITY

REGULATORY OBJECTIVE:

TO PROTECT THE STATE AND ITS CITIZENS AGAINST ALL KINDS OF NATIONAL CRISES

TRADE POLICY

REGULATORY OBJECTIVE:

TO PROMOTE FREE TRADE AND MARKET ACCESS WHILE RECOGNISING THE RIGHT TO REGULATE TO PROTECT SAFETY, HEALTH, ENVIRONMENT AND NATIONAL SECURITY

gear used in ordinary life and business, such as smart phones, computer programs, firewalls, smart devices, operating systems and smart cards, have connections to critical infrastructure, such as, for example, transportation, banking and health systems. These sectors are vital to the functioning of our society and need to be protected from all kinds of hazards and disturbances.

We could presume that there exist effective, coordinated and harmonised paths to address IT security in ICT products based on international frameworks and standards. In practice, however, regulators in different countries use their own national strategies to address IT security and often introduce their own national requirements on top of, or as an alternative to, existing international standards, arguing that they face specific national security concerns. Examples of such regulatory measures include preferences for national standards or specific national certification requirements that often result in duplicative and costly procedures for businesses. Accordingly, the approaches taken by regulators in the field of IT security are characterised by specific national concerns, with security as a priority, rather than measures that follow international standards and commitments regarding trade and market access.

This development is by no means remarkable. To protect one's own infrastructure from incursion and to avoid vulnerabilities, it could actually be necessary to conceal possible paths to classified and protected information from outsiders by using specific rather than common approaches. Unfortunately, as with any regulation of industrial products, differing national requirements (in the case of IT security often partially concealed and not transparent) risk becoming barriers to international trade. The value of having open regulatory processes and transparent regulations, as is the case in most other product areas, is that it allows businesses to provide input to regulation (e.g., in standardisation) and to quickly understand and compare what regulation applies in various markets and why.

The regulators may approach enhanced IT security in various ways. It is possible to prepare mandatory requirements for the properties of ICT products themselves. This approach carries a risk however that rapid technological development can make such regulations very quickly obsolete.

A more common and widely used strategy is to prepare requirements on conformity assessment, i.e., how ICT products are certified. Although there are international standards and schemes for cybersecurity certification, these standards and schemes are rather generic. This low specificity results in various degrees of gold plating, where regulators in different countries introduce additional national requirements on top of the international standards in order to address national security. In practice, these additions mean that the IT security requirements for the same ICT product can be different in different countries. The exact requirement level chosen is to a high degree dependent on how authorities perceive the risks and vulnerabilities in their country.

At the same time, the number of technical barriers to trade (TBTs) within the World Trade Organisation (WTO) is increasing. Further economic sanctions (or threats of sanctions) related to IT security are more frequently raised at the negotiation tables by leaders in world trading powers. These developments clearly signal that IT security has also become a concern for trade policy.

Even though barriers related to IT security have been discussed within the WTO, none of the cases have advanced to formal dispute settlement. This is probably because national security is an extremely delicate and difficult subject to address from a legal point of view. The result is that businesses experiencing problems with market access actually need to adapt to the situation.

International standards and schemes for improved regulatory coherence in the field of IT security do exist. This work has even resulted in mutual recognition of IT security certificates in some areas. The problem is that various markets apply these mechanisms differently, for exam-

ple, by introducing additional requirements on the top of international standards. Accordingly, existing international regulatory cooperation between countries might well address IT security but does not, for the time being, necessarily suffice to contribute to smooth market access across borders for ICT products. A severely fragmented IT security landscape established by nations to protect themselves may also ultimately result in less secure products and services.

Policy makers are successively becoming aware of regulatory fragmentation and that the need to address IT security is becoming increasingly urgent. As a result, new policies and legislative tools are underway to create greater international harmonisation. This change could result in greater openness and transparency, promoting international trade. In the best scenario, the preparation and adoption of harmonised requirements for IT security would move from closed to open fora. This would allow various stakeholders to gain more insight into and have a greater voice with respect to potential regulatory outcomes. Increased harmonisation would also benefit businesses as it could reduce or abolish unnecessary costs from different and duplicative requirements in various markets. Further, this change would make it possible to streamline IT security requirements for ICT products based on actual vulnerabilities and risks. Using this approach would make the rationale of the regulations easier to understand. This change would also potentially reduce costs to society and the end-users paying for IT security measures.

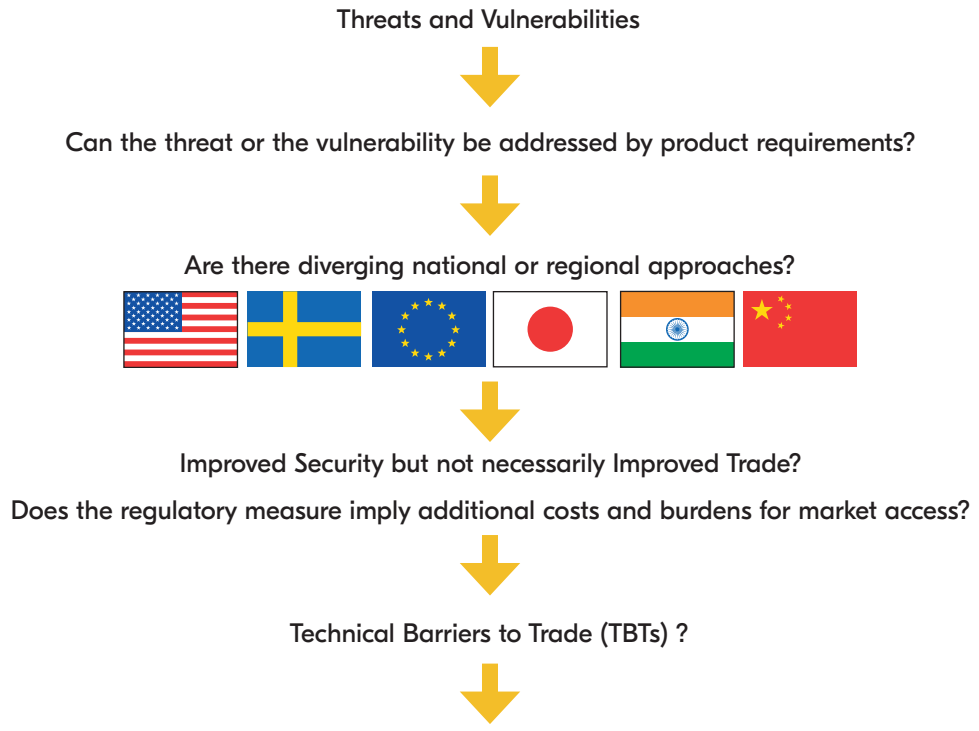
Important regulatory instruments affecting ICT products within the European Union are the eIDAS (Regulation on electronic identification and trust services for electronic transactions in the internal market), the NIS Directive (Directive on security of network and information systems) and the Cybersecurity Act (under negotiation). The latter, in particular, focuses on finding more harmonised schemes for conformity assessment, i.e., cybersecurity certification of ICT products. At the same time, many IT security experts are hesitant about the value of comprehensive and costly product certifications. Certifying a product does not make it safe (i.e., a certification does not necessarily remove all vulnerabilities) - the risks are to a high degree dependent on where the ICT product is used. Comprehensive certification with high assurance levels might thus represent considerable market value; but ultimately, suppliers and consumers will pay the cost.

Due to the complexity and the cost, the number of cyber security certifications are rather small in relation to the number of ICT products and development processes that would need to pass certification to create improved security for society. As a result, regulatory strategies are increasingly shifting from securing products to securing the IT infrastructure in which the products are used. In practice, this means that instead of preparing requirements on the properties of commercial ICT products themselves, requirements are established for the platform that are used to send data. This change may concern IT platforms within a certain sector or between public agencies where various ICT products are used. This approach does not make the regulation of products irrelevant. Instead, this approach improves overall security, as it takes into account the vulnerabilities presented by commercial products from the very beginning.

The benefit of an approach focusing on infrastructure is that authorities may find a more systematic and harmonised way to effectively address IT security on the national level while at the same time allowing market access to commercial ICT products that are certified according to international standards. Therefore, there are better possibilities to maintain and improve IT security without creating new TBTs. As this solution implies investments in new infrastructure, public bodies need to evaluate the costs and benefits of the solution, taking into account specific risks for the sector in question. For this national approach to work, the connected product requirements for certification also need to be based on international standards. If other standards are decided upon and made mandatory regionally (e.g. in the EU), businesses might still end up with duplicative, expensive certifications and, consequently, face the risk of trade barriers.

Within the framework of this report, business representatives have strongly underlined the global character of the ICT market. Companies are especially wary of regulatory harmonisation not taking into account sector specific differences. These aspects motivate a thorough discussion of new regulatory initiatives in the field of IT security.

Figure 1. IT security regulation- issues to consider



The main conclusion of this report is that there is a need to increase knowledge of IT security at all levels of society. Based on the analysis, it is not necessarily the individual technical barriers that need to be focused upon; it is the lack of trust in different regulatory strategies that may generate unnecessary costs and reduced security.

It is vital, therefore, that policy makers grasp the breadth and effect of cyber threats in our society. An essential factor is to take note of the interdependencies between societal infrastructure concerns (national security policy) and trade (trade policy) when addressing IT security. It is crucial to understand the limitations, shortcomings, interdependencies and effects of different regulatory alternatives with respect to market access at the national, regional and international levels.

All too often, attention to IT security is focused on technical solutions. To address IT security in ICT products, it would, however, be valuable to first analyse the possible threats (e.g., confidentiality, availability, integrity), motives (e.g., money, power, ideology), stakeholders, targets (citizens, businesses, public sector, societies, nations) and tools (e.g., ransomware, phishing, tailgating, DoS attack). Such an assessment would better support decisions regarding what kind of regulatory measures and requirements are relevant and justifiable to secure information. The risk scenarios and actions for IT security are most likely different for a company in manufacturing, for a public railway system, or for a powerful political think tank forming public opinion.

Furthermore, IT security is not about a static technology; it is about processes in constant change. As technologies advance, so do the user environments and parameters that affect IT security for ICT products. Therefore, legislation will have less value in addressing problems compared to many other areas. Additionally, stakeholder motives and actions are difficult to detect, identify and address.

The effects of these developments manifest, for example, in that countries ban ICT procurement from other nations, resulting in markets closing themselves to trade. Resistance against cybersecurity threats could also be signalled by using economic sanctions (or the threat of them) and export control measures. If these trends continue, traditional trade policy instruments might fail to be effective. The handling of security concerns could in the future be dependent on bilateral gentlemen's agreements between economic powers. Such a result would deviate from our existing trade patterns and risk further undermining multilateral trade policy processes.

It is important to understand that IT security is to a high degree a policy challenge. The best way to address IT security is to increase competence by contributing to a holistic approach to the matters involved. In addition, it is essential to closely monitor and openly debate new regulatory policies and approaches for IT security. A decisive component here is to create trust, both between stakeholders and in the regulatory solutions, especially regarding market access and international trade in ICT products.

Sammanfattning

Syftet med denna utredning är att redogöra för konceptet IT-säkerhet. Syftet är också att beskriva hur IT-säkerhet i informations- och kommunikationsteknologi (IKT) kan regleras samt belysa vilken inverkan denna reglering har på produkternas marknadstillträde och internationell handel. I utredningen diskuteras vidare om en ökad harmonisering av regler för IT-säkerhet i IKT är möjlig, särskilt då det är uppenbart att befintliga regleringsstrategier präglas av nationella särintressen snarare än försök till samordning och internationella åtaganden.

Denna utredning visar att reglering av IT-säkerhet i IKT är ett komplext område som inte följer samma struktur och logik som varureglering generellt. Utredningen åskådliggör vidare att politiska beslut avseende IT-säkerhetsreglering har en betydande bäring, inte endast på säkerhet, utan även på internationell handel.

Även om digitalisering bidrar till en stor effektivisering i vårt samhälle har det blivit uppenbart att den teknologi som vi använder för att kommunicera och dela information också för med sig allvarliga sårbarheter. Dessa sårbarheter uppenbarar sig i cyberhot eller cyberincidenter, obehörig tillgång till information, förlust eller stöld av information eller störningar i verksamhet. Detta gör IT-säkerhet till en av de viktigaste frågorna i vårt digitaliserade samhälle.

Beslutsfattare och myndigheter som ska ta ställning till IT-säkerhetsreglering behöver ha förståelse för att samhällets funktion vilar på ett stort antal strukturer som är sammankopplade och beroende av varandra, och där det är omöjligt att skilja cyberrymden (som en egen domän) från t.ex. sektorer som livsmedel, hälsa och transport. Cyberrymden kan ses som ett tunt nät som går igenom alla sektorer och som gör att sektorerna kan fungera och kommunicera med varandra. Områden som är i riskzonen för cyberincidenter och -attacker är t.ex. företag, smarta städer, smarta hem, energisystem, järnvägar, flyg, smarta elnät och myndigheter. Det bör vidare uppmärksammas att vårt sätt att leva och handla varor baseras på globala snarare än på lokala förhållanden, vilket också måste tas i beaktande vid reglering av IKT som tillverkas, säljs och installeras runt om i världen.

Det finns flera sätt att bidra till en höjd IT-säkerhet. En metod är att ställa krav på IKT genom lagstiftning. IT-säkerhetsregler för IKT skiljer sig dock markant från annan varureglering eftersom dessa regler inte bara måste beakta hälsa, säkerhet och miljö, utan också samhällets infrastruktur, den personliga integriteten och nationell säkerhet. Detta på grund av att IKT, som smartmobiler, dataprogram, smarta apparater, brandväggar, operativsystem och smartkort inte bara används i hem och på arbetsplatser utan även inom sektorer som ingår i kritisk

IT-säkerhetsreglering som policyutmaning

NATIONELL SÄKERHET

REGULATIV MÅLSÄTTNING:

SKYDDA STATEN OCH DESS INVÅNARE MOT ALLA TYPER AV NATIONELLA KRISER

HANDELSPOLITIK

REGULATIV MÅLSÄTTNING:

BEFRÄMJA FRI HANDEL OCH MARKNADSTILLTRÄDE OCH SAMTIDIGT ERKÄNNA RÄTTEN ATT REGLERA FÖR ATT SKYDDA SÄKERHET, HÄLSA, MILJÖ OCH NATIONELL SÄKERHET

infrastruktur, såsom transport, banker och hälsovården. Dessa sektorer är nödvändiga för att vårt samhälle ska kunna fungera och måste skyddas mot sårbarheter och störningar.

Eftersom IT-säkerhet är en så kritisk och samhällsgenomgripande fråga förmodar vi kanske att sätten att säkerställa IT-säkerheten är effektiva och internationellt koordinerade och standardiserade. I praktiken är det dock så att myndigheter och regelgivare i enskilda länder antar egna metoder och strategier för att hantera IT-säkerhet. Myndigheter inför ofta specifika, nationella regler som kompletterar, eller som fungerar som ett alternativ till, befintliga internationella standarder. Detta motiveras med att det finns särskilda nationella säkerhetsbehov. Dessa nationella standarder eller certifieringskrav leder till att företag måste genomgå certifieringar i flera länder, vilket leder till ökade kostnader. Man kan konstatera att de åtgärder som myndigheter tar idag när det gäller IT-säkerhet karakteriseras av specifika nationella behov med säkerhet som prioritet, snarare än åtgärder som följer internationella standarder och åtaganden om beaktar handel och marknadstillträde.

Denna utveckling, där åtgärder för nationell säkerhet prioriteras på bekostnad av handel och varors marknadstillträde, är ingalunda överraskande. Det är naturligt att vilja dölja vägar till hemligstämplad eller skyddsvärd information från utomstående genom att tillämpa specifika snarare än allmänt kända tillvägagångsätt. Men konsekvensen av sådana nationella regler (som när det gäller IT-säkerhet ofta är icke-transparenta) blir densamma som för reglering inom andra områden, dvs. en regulativ fragmentering som riskerar skapa handelshinder. Genom detta beteende förloras värdet av öppna regulativa processer och transparenta regleringar som gör att företag har en möjlighet att påverka regleringar (t.ex. inom standardisering) och att de snabbt kan förstå och jämföra vilka regler gäller på olika marknader och varför.

Myndigheter kan anta olika strategier för att höja IT-säkerheten på varor. En strategi är att utarbeta tekniska föreskrifter med bindande krav på egenskaper i IKT. Här finns dock en stor risk att den tekniska utvecklingen snabbt gör reglerna föråldrade.

En annan strategi som används mer utbrett är att ta fram regler för så kallad bedömning av överensstämmelse, dvs. hur IKT ska certifieras. Fastän det finns internationella standarder och ordningar för cybercertifiering är kraven i dessa relativt generiska. Detta leder till att olika länder tar fram egna nationella krav som kompletterar internationella standarder. Detta innebär att kraven för en och samma IKT-produkt kan skilja sig åt i olika länder, beroende av hur myndigheterna ser på risker och sårbarheter i sitt land.

En konsekvens av att nationella särkrav ökar är en risk för tekniska handelshinder. Man kan notera att antalet tekniska handelshinder som rör IT-säkerhet och som diskuteras inom Världshandelsorganisationen (WTO) har blivit fler på senare år. Det blir också allt vanligare att ekonomiska sanktioner (eller hot om sanktioner) relaterade till IT-säkerhet lyfts upp på förhandlingsbordet när stormaktsledare möts. Denna utveckling är en tydlig signal på att IT-säkerhet även blivit en fråga för handelspolitiken.

Man kan också konstatera att även om ett antal handelshinder avseende IT-säkerhet har diskuterats inom WTO, så har inga av dessa hinder tagits upp till tvistlösning. Skälet för detta är förmodligen att nationell säkerhet är en känslig och svår fråga att hantera från ett rättsligt perspektiv. Denna situation leder dock till att de företag som möter hinder inte får någon rättelse utan är tvungna att anpassa sina produkter till de nationella kraven.

Som redan nämnts saknas inte internationellt regulativt samarbete. Med andra ord finns det internationella standarder och ordningar som ska bidra till ökad regulativ samstämmighet inom IT-säkerhet internationellt. Några av dessa ordningar har till och med lett till att nationer ömsesidigt godkänner certifikat inom vissa områden. Problemet är, som tidigare nämnts, att olika marknader tillämpar dessa standarder olika, bl.a. genom att lägga till egna krav som ett komplement till internationella standarder. Detta innebär att ökat internationellt regulativt samarbete visserligen kan bidra till höjd IT-säkerhet, men att arbetet inte nödvändigtvis bidrar till en

fungerande gränsöverskridande handel med IKT. En fragmenterad global marknad, där olika länder skyddar sig själv genom nationella regler, kan tyvärr också leda till mindre säkra produkter och tjänster. Detta genom att resurser som skulle ha kunnat användas för god regleringssed som är accepterad och gångbar internationellt används för att ta fram olika nationella särlösningar.

Beslutsfattare har successivt blivit mer medvetna om den ökande regulativa fragmenteringen på IT-säkerhetsområdet och inser att situationen kräver kraftiga och skyndsamma åtgärder. Detta har lett till nya politiska initiativ och förslag på lagstiftning med syfte att öka internationell harmonisering.

En ökad internationell harmonisering skulle kunna leda till större öppenhet och transparens, och befrämja internationell handel. I bästa fall skulle utformningen av IT-säkerhetsregler flyttas från slutna till öppna grupper, vilket skulle ge olika intressenter större insyn i regleringsprocessen och en möjlighet att påverka utfallet. En ökad harmonisering skulle också göra så att företag kunde slippa onödiga kostnader förknippade med anpassning till olika och duplicerande krav på skilda marknader. En harmonisering skulle vidare göra det möjligt att strömlinjeforma krav på IT-säkerhet för IKT så att kraven speglar verkliga sårbarheter och risker. På detta sätt skulle krav på IT-säkerhet också bli mer tillgängliga och lättbegripliga för företagen. Ökad harmonisering skulle därutöver ha potential att sänka kostnaden för samhället och konsumenterna som betalar för IT-säkerheten.

Inom EU utgör eIDAS-förordningen (förordningen om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden), NIS-direktivet (direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen) och Cybersäkerhetsakten (förslaget till förordning om ENISA, EU:s cybersäkerhetsbyrå, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik, under förhandling) viktiga rättsakter och politiska initiativ som påverkar IKT. Särskilt Cybersäkerhetsakten har som målsättning att bidra till mer harmoniserade ordningar för bedömning av överensstämmelse, dvs. för cybersäkerhetscertifiering av IKT. Samtidigt är många IT-säkerhetsexperter tveksamma till värdet av omfattande och dyra produktcertifieringar. En certifiering gör nämligen inte en produkt säker (dvs. en certifiering avlägsnar nödvändigtvis inte alla sårbarheter), eftersom riskerna framför allt är knutna till den miljö där IKT används. Omfattande certifieringar kan således generera ett högt marknadsvärde men i slutändan är det leverantörer och konsumenter som får stå för notan.

Genom att produktcertifiering är komplext, tidskrävande och dyrt är antalet certifieringar relativt få i förhållande till antalet IKT och produktutvecklingsprocesser som borde genomgå certifiering för att skapa säkerhet i samhället i stort. Som en konsekvens av detta har det skett en förändring i regulativa strategier; i stället för att säkra själva produkten har fokus skiftat till att säkra den IT-infrastruktur där produkten används. I praktiken innebär detta att man ställer krav på de plattformar som används för att skicka information och där IKT används. Detta kan omfatta IT-infrastrukturer inom en viss sektor eller mellan ett antal myndigheter. Detta tillvägagångssätt avskaffar inte behovet av produktreglering men den höjer säkerheten i stort, genom att metoden från första början tar hänsyn till risker som finns och kan kvarstå hos kommersiella produkter trots certifiering.

Fördelen med en strategi som fokuserar på IT-infrastruktur är att myndigheterna kan hitta ett mer systematiskt och harmoniserat sätt att effektivt adressera IT-säkerhet på nationell nivå och samtidigt kunna godta kommersiella varor som är certifierade enligt internationella standarder. På detta sätt finns det förbättrade möjligheter att höja IT-säkerheten utan att skapa nya tekniska handelshinder. Eftersom denna metod kräver investeringar i ny infrastruktur är det nödvändigt att utvärdera kostnader och fördelar utifrån sektorsspecifika risker.

Det förtjänas dock att betonas att för att IT-infrastrukturstrategin ska fungera, måste produktkraven avseende certifiering baseras på internationella standarder. Om myndigheterna tilläm-

par eller gör andra regionala standarder bindande (t.ex. inom EU), kan det leda till att företag drabbas av duplicerande och dyra certifieringar, dvs. riskerar handelshinder.

Företag som vi har haft kontakt med i samband med denna utredning har betonat att IKT-marknaden är global och att det således krävs internationellt accepterade lösningar för reglering. Representanter för näringslivet anser också att initiativ som strävar efter regulativ harmonisering måste beakta skillnader som finns mellan olika sektorer. Dessa aspekter motiverar en noggrann analys av nya regulativa initiativ avseende IT-säkerhet.

Figur 1. Frågeställningar kopplade till reglering av IT-säkerhet

Huvudslutsatsen i denna rapport är att det finns ett stort behov att öka kunskapen om IT-säkerhet i samhället. Analysen tyder på att inte är de enskilda handelshindren som nödvändigtvis ska stå i fokus, utan avsaknaden av tillit för olika regulativa strategier som kan generera onödiga kostnader och sämre säkerhet.

Det är viktigt att beslutsfattare förstår både omfattningen och effekterna av cyberhot. Det omfattar beroendeförhållandena som finns mellan samhällets infrastruktur (nationell säkerhet) och handel (handelspolitik) när man vidtar regulativa åtgärder för att höja IT-säkerheten.

IT-säkerhet för alltför ofta vårt fokus till tekniska lösningar. Men för att hitta en relevant metod för att reglera IT-säkerhet i IKT vore det värdefullt att först analysera möjliga hot (t.ex. konfidentialitet, tillgång, integritet), motiv (t.ex. pengar, makt, ideologi), intressenter, mål (medborgare, företag, statliga sektorn, länder) och verktyg (ransomware- utpressningsprogram/virus, phishing -nätfiske, tailgating - obehörig passering, DoS attacker-överbelastningsattacker). En sådan undersökning skulle bättre underbygga beslut om vilka regulativa åtgärder och krav är relevanta och försvarbara för att säkra information. De riskscenarion som finns för IT-säkerhet är förmodligen olika för t.ex. för en tillverkare, för en statlig järnväg eller en mäktig politisk tankesmedja med syfte att påverka allmänhetens åsikter.

IT-säkerhet handlar inte om statisk teknik utan om konstanta förändringsprocesser. Genom att tekniken utvecklas, utvecklas också användarmiljön och de variabler som påverkar IT-säkerhet i IKT. Därför är det viktigt att inse att lagstiftning inom IT-säkerhet har mindre effekt än på många andra regleringsområden. Detta är även kopplat till att olika intressenters motiv och agerande mycket svåra att upptäcka, identifiera och hantera.

Den snabba IT-utvecklingen och de ökande cyberhoten leder till att vissa länder förbjuder eller begränsar sin import av IKT från andra länder vilket innebär att länderna sluter sina gränser för handel. Ett motstånd mot cyberhot kan också komma till uttryck i att länder använder sig av ekonomiska sanktioner (eller hot om sanktioner) eller exportkontrollåtgärder. Ifall dessa trender består är det mycket möjligt att handelspolitiska verktyg som lagstiftning och internationella avtal kommer bli ineffektiva. Framtidens hantering av IT-säkerhetsincidenter kommer kanske i större utsträckning baseras på muntliga avtal mellan ekonomiska makter. En sådan situation skulle vara olycklig i det att den avviker från vår nuvarande handelspraxis och riskerar att ytterligare underminera multilaterala handelspolitiska processer.

IT-säkerhet är framför allt en policyutmaning. Det bästa sättet att möta utmaningen är att höja kunskapen i samhället, och för beslutsfattare och myndigheter att försäkra sig om att de har en helhetsbild om de frågor som är kopplade till policyåtgärder inom området. Utöver detta är det viktigt för experter, beslutsfattare och företag att noggrant bevaka, och öppet diskutera olika regulativa angreppsätt och åtgärder för att höja IT-säkerheten. En avgörande faktor för marknadstillträde och internationell handel med IKT är att ökat förtroende kan byggas mellan både länder och regelgivare samt för olika regulativa alternativ.

Contents

1 Introduction

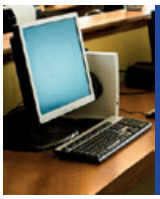
Globalisation, new trading patterns and innovations reflected in new technologies and products are all linked to effective information sharing. The benefits of a digitised society manifest in the cost effectiveness and almost unlimited possibilities to communicate and share information. At the same time, the existing infrastructure, platforms and products supporting information flow leave us extremely vulnerable.[1] Each component in the Information and Communication Technology (ICT) infrastructure may be affected by unintentional damage as well as targeted sabotage.[2]

A lack of strategies to address IT security may result in severe disturbances affecting all of society. In a world connected by digital networks and trade networks, it will not be sufficient to protect only yourself. IT security is a global challenge, which demands coordinated approaches, particularly now that trade policy scene is threatened by turbulence and protectionist tendencies.[3] The governments of individual countries face a dilemma however. On one hand, massive investments in ICT infrastructure are made to boost services and competitiveness, and on the other hand, this technological expansion results in new risks that are very difficult to control. In other words, our society becomes more effective but increasingly vulnerable to cyberattacks.[4]

For the common citizen, IT security most frequently manifests as the hijacking of an e-mail account, loss of data, or a system failure on a personal computer.[5] News of hacker attacks affecting public agencies successively create more awareness of the vulnerabilities presented by technologies and the systems used. Political instability worldwide may also draw attention and make people realise the possible threats presented by terrorism related to products and systems that are available and used every day.[6]

As private persons, we most often happily leave the security of our gadgets to the experts. At the same time, the products we increasingly use in our daily lives are designed, manufactured and distributed online. These same devices are also used in environments that are critical for security, which creates entirely new regulatory challenges for society as a whole.[7] An example of such aregulatory challenge is a case where the definition of a product and service are blurred, such as for 3D

Figure 2. Different levels of regulation



Requirements on products

Requirements on conformity assessment, (certification of development process or product)

Requirements on the infrastructure where products are used

Value of Cyber

- 90% of global population will be Internet users by 2030.
- World population 7.6 bn, IoT devices 8.4 bn (20bn or more in 2020).
- Valuable, operation critical information and data are commonly uploaded in the cloud today.
- Global costs for cybercrime damages are set to double to 5,1tn EUR by 2021.
- Economic impact of cybercrime in the EU is estimated to be more than 55bn EUR per year.
- Complexity of attacks and sophistication of malicious actions in cyberspace increase, and attackers are getting better at hiding their trails.
- State backed attacks are on the rise.
- In the EU telecommunications sector alone, in 2016, 158 significant incidents were reported.
- Top 15 threats identified in the EU are malware, web-based attacks, web application attacks, phishing, spam, denial-of-service, ransomware, botnets, insider threats, physical manipulation/damage/theft/loss, data breaches, identify theft, information leakage, exploit kits and cyber espionage.
- The value of the global cyber market is estimated to be 605bn EUR.
- The number of global cybersecurity related companies is 222k.
- The value of the EU cyber market is estimated to be 158bn EUR.
- The number of EU cybersecurity related companies is 60k.
- The cyber security market sub sector leaders are in the field of situational awareness, infrastructure, application security, system recovery and data cleansing, business continuity, identity and access, anti-malware, cyber security insurance, mobile, encryption, cyber consultancy outsourced services and training and education.

Please note: Figures on cyber (comparing attacks/espionage/incidents) should be evaluated critically, as data do not cover all vulnerabilities risking or causing disturbances or harm overall.

Sources: CIMA, Cybersecurity Industry Market Analysis 2018; ENISA, Annual Incident Reports 2016, 2017; Lee- Makiyama, Stealing Thunder, 2018; Trocmé & Banktander, Cybersecurity, 2019; World Economic Forum, The Global Risk Report, 2018.

Technical Barriers to Trade (TBTs)

Technical requirements on products can in certain circumstances result in unnecessary obstacles to international trade, so called **technical barriers to trade (TBTs)**. The preparation, adoption and application of technical requirements are regulated by the WTO Agreement on Technical Barriers to Trade (TBT Agreement). The aim of the TBT Agreement is to ensure that product requirements and procedures used to assess compliance with those requirements do not create unnecessary obstacles to international trade.

technology. Such a case entails consideration of the level at which IT security should be regulated, especially in order to detect societal infrastructure concerns and trade effects:

- Should the regulator set requirements on ICT products themselves and/or on the conformity assessment of products, i.e., certification?
- Should the regulator prepare requirements related to IT infrastructure where products are to be used?

These regulatory paths are explored in more depth in Chapter 4.

For businesses, sustainable and secure solutions are vital, as cyberspace is international and characterised by interdependencies. Therefore, most sectors are dependent on interconnected and interdependent infrastructures. ICT has become an essential component in the everyday operations of critical sectors such as transportation, food and health, including the infrastructure that support them. This situation creates a demand for regulatory approaches to ICT products that consider the interdependencies and provide for smooth market access globally.

When individual countries invest in digitalisation and new technologies, such as the production of telecommunications equipment, and increase IT security requirements, these requirements risk becoming TBTs. These barriers may concern product requirements based on national standards, a certification requirement based on national standards, requirements based on national standards for encryption, or local manufacturing requirements that effect other countries' ability to export products.

The justification for TBTs[8] related to IT security that has already been discussed in the WTO TBT Committee[9] is national security.[10] Therefore, countries have defended their regulatory measure by referring to national security, which is a regulatory objective considered legitimate by the WTO.[11]

IT security and national security exceptions within the WTO (i.e., the deviation from regulatory principles promoting international standards and practices and instead choosing national approaches for regulating goods based on national security interests)[12] have been widely studied by academics from a legal point of view.[13] For instance, many efforts have been made to evaluate whether countries violate international trade policy commitments if they adopt national IT security requirements that diverge from international standards. So far, however, none of the TBTs discussed at the WTO TBT Committee have been brought to formal dispute settlement. Additionally, the practice of the General Agreement on Tariffs and Trade (GATT) and the Agreement on Technical Barriers to Trade (TBT Agreement) are inconclusive on the issue of national security.[14] Therefore, countries and businesses that face trade barriers actually need to adapt to existing market conditions without receiving any remedy for the additional costs or denial of market access they might face, which is quite extraordinary. This result is obviously due to conflicts between trade and security policies. Further unilateral declarations about legitimacy on this delicate matter would set a dangerous precedent for IT security exceptions.

Critical infrastructure?

Defining critical infrastructure is political and depends on national policies and priorities. In general, critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy.

The U.S. has identified 16 sectors that constitute the critical infrastructure that more or less correspond to the areas pointed out in the directive on security of network and information systems (NIS Directive) in the European Union: chemicals; commercial facilities; communications; critical manufacturing; dams; defence industrial bases; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportations systems; waste and wastewater systems.

When regulating within critical infrastructure, like transportation or financial services, regulators need to regard both the requirements for the platforms that are used for sending data within the sector (IT infrastructure) and the requirements for ICT products that are used within the IT infrastructure (mobiles, computers, equipment, devices, vehicles etc.).

It is probable, however, that new TBTs will continue to appear unless countries work to create common regulatory principles to address IT security for ICT products. This is more important now than ever, especially as the world's giant trading powers seek enhanced regulatory coherence by comprehensive and far-reaching free trade agreements (FTAs).[15] In FTAs, the parties try to agree on common ways to regulate certain product areas and sectors in order to prevent or abolish TBTs.

One of the initial issues in addressing regulatory harmonisation in the field if IT security is whether it is possible and useful to try to differentiate between critical[16] and non-critical infrastructure in order to reach agreement on the level of transparency and the regulatory approach for IT security in ICT products.

In other words, the question is whether the same or similar requirements on IT security are applicable for all types of ICT products.

The answer to this question is not straightforward, which also makes the regulation of IT security a multifaceted challenge. Drawing the line between national security and other domains defines the technologies embraced and indicates to what extent a country may or must rely on its infrastructure.[17]

The approaches taken naturally vary between countries. A country might wish, for example, to limit or ban foreign countries acquiring or operating mobile networks. In such case, the approach implies national control of networks, which makes the securing of components (ICT products used within the network) less important. Another country might not be able to protect networks, which shifts the interest and requires securing the components (ICT products) involved. Similarly, railway systems may be considered a national security resource depending on the importance and use of the system (e.g., transportation of nuclear weapons). Another country might not have any military defence but might be very dependent on a functioning financial sector and so on.

In many cases, public bodies and specialised agencies with responsibility for IT security are connected to national security. These entities do not therefore necessarily focus, or may not even have the mandate to focus, on the trade aspects of regulations. When preparing infrastructure-critical requirements, security authorities may even see additional national requirements as prerequisites for protecting national security.[18]

The lack of transparency in national IT security regulation means that it will be difficult to create understanding and trust in the regulation of IT security for ICT products globally, because various stakeholders have difficulty getting insight into, participating in, and possibly providing comments on draft regulations and standards for security issues affecting ICT products.[19] In other words, a risk owner will have difficulty relying on standards or certification schemes without transparency and the possibility of influencing the regulations in a way that incorporates his/her own

needs. Often, this situation results in new closed groups regulating a specific area in their own interests. The consequence will be regulatory fragmentation, which, in turn, creates trade barriers and costs for suppliers and consumers.

Current policies for IT security regulation might also not address reciprocity, that is, nations should perhaps analyse the logic of expressing concerns about the regulatory measures of other nations in relation to their own regulatory principles. It would also be beneficial for policy makers and regulators to actually acknowledge the specific technological and cultural challenges in addressing IT security in other countries that differ from their own.

1.1 The rationale of the analysis and its limitations

The objective of this report is to describe the function of IT security, to define by which means IT security in ICT products can be regulated and to highlight in which manner the regulation of IT security has a bearing on trade and market access internationally. This analysis will form a framework in which the regulation of IT security for ICT products can be debated given the number of policies and interlinkages that have a bearing on the subject.

The ambition of this report is also to discuss whether the diverging national strategies in the field of IT security regulation could be harmonised to a greater extent. An important element here is to highlight the need for better understanding and coordination between national security policy and trade policy in the field of IT security regulation of ICT products. Such knowledge as well as joint efforts could prevent increased regulatory fragmentation and unnecessary barriers to international trade.

The analysis does not intend to evaluate to what extent diverging national requirements on IT security creating trade barriers conflict with international trade policy commitments. Nor is the objective of the analysis to provide recommendations on the exact paths to address IT security for ICT products with security features. It is obvious that systems and structures are likely to differ from one area and product sector to another, depending on different risk scenarios. Instead, the analysis has a practical approach; the discussion will focus on existing regulatory tools, alternatives and their effects in order to project the ways forward, taking into account both IT security and international trade.

For this analysis, it would have been interesting to present case studies highlighting the approaches and challenges of government and business in various countries and sectors. The delicacy of the subject matter, the lack of transparency in regulation and the differences between various sectors and product areas, however, made such an analysis impossible.

The analysis needs to embrace the fact that parts of IT security regulation regarding indus-

IT security- terminology

The terms information security, computer security, information assurance and cybersecurity are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity, availability and traceability of information. There are, however, some subtle differences among them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.

In this report the term **IT security (sometimes Cybersecurity)** will *mainly* be used, depending on when references are made to established areas and concepts, such as the cybersecurity strategy of the European Union or when discussing requirements on conformity assessment (testing, certification and accreditation), when the term cybersecurity certification is used. For clarifications of terminology, see the Glossary.

trial goods are still regarded as a strict national interest by individual governments. It is, therefore, not necessarily a primary subject of international trade harmonisation efforts. The analysis will also have to consider that opinions on IT security regulation vary to a high degree among the main stakeholders, namely, the security agencies, regulators, businesses and policymakers, and depends greatly on their insight and interest in the rather delicate subject matter.

The creation of a bridge between national security and trade policy is already ongoing. More recent legislative measures in Europe such as the NIS Directive and the proposal for an EU Cybersecurity Act[20] clearly acknowledge the need to address IT security from a societal infrastructure (national security) perspective as well as from the market access (trade policy) perspective.

The analysis also acknowledges that IT security regulation has substantial effects on domains such as intellectual property rights (IPR)[21] and services, but it focuses on the technical regulation of industrial goods falling under the TBT Agreement.

1.2 Outline

The report will embark on a discussion of the concept of IT security in general. An effort is made to try to define how the IT security regulation of ICT products is and is not related to trade policy (Chapter 2). The objective is to highlight the root of the problem, namely, that IT security regulation is to a high degree based on the requirements and principles set in national security policies by security agencies and authorities.[22] These requirements do not necessarily match the demand for assurance stemming from technological development and digitalisation overall.

The analysis will continue by focusing on one path to addressing IT security, i.e., the technical regulation and especially the requirements for conformity assessment, which include certification requirements for cybersecurity in ICT products (Chapter 3). The motivation for this approach is that such requirements have resulted in TBTs and have been addressed within the international trade policy arena in the WTO. A more comprehensive analysis of cybersecurity certification also contributes to the understanding of the complexities in ongoing regulatory initiatives in the EU.

The discussion will continue by highlighting existing regulatory mechanisms and ongoing regulatory proposals for regulatory harmonisation in Europe and internationally (Chapter 4). Doing so will allow us to reflect upon the source of regulatory fragmentation and challenges within the area of the certification of cybersecurity in ICT products. An attempt is also made to visualise the main regulatory levels and paths addressing IT security regulation, as the mechanisms have a bearing both on security and trade.

The report will conclude with remarks on regulatory harmonisation in the field of IT security and will highlight aspects that need to be considered in policymaking when considering ways forward (Chapter 5).

2 What is IT security?

As a concept, IT security is complex and not necessarily easily understood. In this chapter, the concept of IT security is defined. The objective is also to clarify how and to what extent IT security regulation for ICT products is related to trade policy.

Information inside ICT products and systems is a critical resource that enables businesses and organisations to function. Furthermore, citizens have a reasonable expectation that personal information in ICT products or systems will remain private, available when needed, and not subjected to unauthorised modification.[23]

ICT products and systems should operate in a manner that ensures that they perform their functions while exercising proper control over that information so that it is protected against hazards, such as unwanted or unwarranted dissemination, alteration or loss. The term IT security is used to include the prevention and mitigation of these and similar hazards.[24]

It is necessary to highlight that IT security is not a single technology. Rather, IT security is a strategy comprising the processes, tools and policies necessary to prevent, detect, document and counter threats to digital information. These strategies typically involve both physical and digital security measures to protect data against unauthorised access, use, replication or destruction.[25]

Lack of IT security: threat scenarios

A lack of strategies in the field of IT security can imply many threats, for example, that

- a machine or network resource is unavailable to its intended users (denial-of-service attacks -DoS),
- an unauthorised user gaining access to a computer and the data in it (direct access attack),
- an imposter obtains key pieces of personally identifiable information, such as social security or driver's license numbers, in order to impersonate someone else (identity theft/identity fraud),
- acts of surreptitious listening to private conversations (eavesdropping),
- masquerading as a valid entity through falsification of data (such as an IP address or username) in order to gain access to information or resources that one is otherwise unauthorised to obtain (spoofing),
- malicious modification of products (tampering), malware that does not aim to obtain money from victims but damages or destroys IT systems or even physical assets and infrastructure (cybersabotage) and
- attempts to acquire sensitive information such as usernames, passwords, and credit card details directly from users (phishing).

A number of stakeholders are at risk, such as financial systems, industrial equipment (telecommunications), aviation, consumer devices (smart phones, computers), large corporations (identity theft, data breaches, cyberwarfare (spreading propaganda, sabotage, espionage), automobiles (connected and self-driving cars), government (police and intelligence agency communications, personal records, passports government ID-cards), IoT and medical systems (medical devices).

The main areas covered by IT security are

1) Application Security
2) Information Security
3) Disaster Recovery
4) Network Security
5) End-user education

Application security encompasses measures or counter-measures that are instituted during the development life cycle to protect applications from threats that can come from flaws in the application design, development, deployment, upgrade or maintenance.

Information security protects information from unauthorised access to avoid identity theft and to protect privacy. Major techniques used in this area are a) identification, authentication and authorisation of users and b) cryptography.

Disaster recovery planning is a process that includes performing risk assessments, establishing priorities and developing recovery strategies in case of a disaster.

Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include a) anti-virus and anti-spyware; b) firewalls to block unauthorised access to the network; c) intrusion prevention systems (IPS) to identify rapidly spreading threats, such as zero-day or zero-hour attacks; and d) virtual private networks (VPNs) to provide secure remote access.

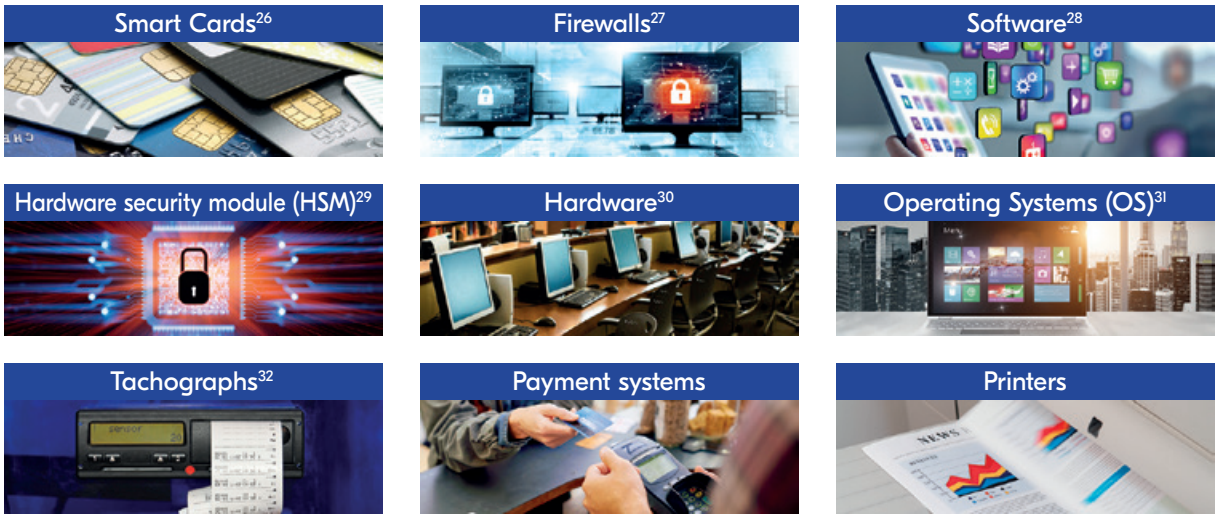
Users have a critical role to play in their organisation's security. Additionally, it is important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This approach may be supported by a systematic delivery of **end-user education**, i.e., awareness programmes and training that deliver security expertise as well help to establish a security-conscious IT culture.

It is fair to argue that there are a multitude of processes, tools, practices and standards for addressing IT security. As many experts have noted, however, policy issues provide a greater challenge than finding a specific technical solution for IT security. Providing a technical interface for various technologies in different countries is relatively easy. Aligning and harmonising the security levels of governmental agencies is a much more difficult task because nations may have very different approaches to addressing cyber threats, even though they could be connected to the same infrastructure and/or use the same products.

2.1 How can IT security for ICT products be addressed?

Before addressing regulatory alternatives, it is necessary to form an understanding of what types of ICT products are subject to IT security regulation.

Figure 3. Some products subject to IT security certification



Some examples are provided in Figure 3 above, although the decisive factor for regulation is not the product category but rather how the product is used and in which environment. Most ICT products are, by default, used equally for communication and information transfer in private homes, businesses, government offices and environments that handle classified or critical information.

It is obvious that preparing clear and effective requirements in the field of IT security is vital for our society. There are, however, several ways of addressing IT security by legislative measures.[33] One route is to prepare requirements for ICT products (with security features) and their certification, including encryption,[34] i.e., by addressing the security in ICT devices and systems themselves. This path is scrutinised in this report with the objective of forming a framework in which the harmonisation of IT security in ICT products can be discussed and analysed like product regulation in other sectors.

Other paths, not explored in this analysis, concern legislation related to public procurement and legislation bearing strictly on national security. Requirements on public procurement are no doubt also interesting for IT security in the field of ICT. However, the domain of public procurement is a complex area falling under another WTO Agreement, namely, the Agreement on

Encryption?

Encryption is an important parameter in creating IT security. Cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages.

The use of encryption is not limited to government and military applications; it has become widespread given its ability to help safeguard the integrity and confidentiality of information. As a result, the great majority of encryption applications involve every day commercial products that are commonly used and traded in the global marketplace. To the extent that encryption is necessary, regulators should note whether regulation favors specific technologies, limits market access or leads to the forced transfer of intellectual property. Further, regulators should acknowledge that technology mandates, including any that involve encryption use in domestic commercial markets, could have significant effects on society and industry that can become outdated, as technologies quickly evolve and thus create interoperability issues.

Common regulatory strategies in this area, especially in areas where Common Criteria certification (see Chapter 3) is not adequate or crypto adapted to critical infrastructure is not available, is important, especially if the aim is to adhere to trade policy principles, such as non-discrimination and transparency. Legal instruments in the EU that make use of encryption for security are regulations on, for example, digital signatures, tachographs and ePassports.

Cybersecurity certification

Being a comprehensive, time consuming and expensive process, cybersecurity certification was earlier known mostly as an area for large security critical products and systems found in the military sector. Digitalisation, technological development and new communication patterns have, however, increased the risks of security incidents fraud, and data breaches in the fields of identification, authentication, digital signatures, payments and connected objects/Internet of things.

In addition, there are growing societal concerns related to privacy and data protection. At the same time, ICT has become the backbone of economic growth and is a critical resource that all economic sectors rely on, leading to the need to ensure an acceptable level of assurance for connected devices in the Digital Single Market and, for example, transatlantic trade flows and infrastructures. Awareness of cybersecurity has thus started to gain well deserved attention, and cybersecurity certification (including encryption) are more of a rule than the exception for ICT equipment, software, smart cards and telecom.

Government Procurement (GPA), which covers only a subset of WTO members[35] and is not the subject of harmonisation efforts like the regulation of goods in general.

Regarding legislation on national security, most regulations targeting, for example, defence (weapons, ammunition, etc.) are clearly outside the scope of trade policy and are a matter of national interest that is not subject to harmonisation. This position is naturally thought provoking as many regulations on IT security are prepared in the domain of national security and have led to a discussion about to what extent regulatory measures concerning ICT could, eventually, be made more transparent and harmonised among countries.

In addition to legislation and mandatory technical regulations, voluntary standards also have a crucial role in a systematic approach to IT security.[36]

These standards will indicate the requirements and guidelines that are useful for all kinds of organisations.[37] With the support of standards, organisations may work based on verified experiences, which provide the premises for improved security.[38]

IT security regulation is scattered over different areas of law. It is necessary to clarify that this analysis focuses on the regulation of industrial goods and the requirements on conformity assessment (i.e., certification). This approach is motivated not only by the importance of requirements on certification of ICT products to address IT security but also by the representation of these requirements as a factual source of TBTs in the global trade policy arena within the Committee for Technical Barriers to Trade in the WTO.[39] These requirements materialise, for example, in requirements for foreign vendors to make their source code[40] available when ICT products are certified,[41] in compulsory registration schemes, in burdensome (domestic) testing requirements and in requirements for use.[42] These regulations have an effect on private businesses, the financial and banking sectors, public transport, energy and telecom, and other sectors that wish to operate in a foreign market.

The role of government is essential when addressing IT security regulation in aninternational context, especially when analysing the implications of the regulation of industrial goods in trade policy. Many stakeholders are sceptical of increasing IT security regulation because regulators may not move fast enough to keep up with cyber threats. However, it is the governments (or WTO members) that need to defend the measures in the WTO if product related requirements end in unnecessary barriers to market access.[43] Accordingly, when security is compromised, governments become accountable.

Without taking an active stance on increasing[44] government intervention in the field of IT security, it must be acknowledged that IT security might not develop by itself in all areas,[45] especially as methods for assessing security, such as certification, involve quite an investment.[46] Furthermore, voluntary arrangements, standards and codes of practice cannot be addressed in the WTO, irrespective of their market impact and value. Hence, a focus on governmental rulemaking is important.

A severely fragmented IT security landscape, established by nations to protect themselves, may ultimately result in less secure products and services, as vendors need to spend significant amounts of resources and money in certifying their products against a multitude of overlapping national cybersecurity standards. These resources could otherwise be spent on improving the security of the products in the first place.

2.2 IT security regulation: compatibility between national security and trade policy

The analysis of the IT security landscape clearly signals that IT security regulation is an issue in several policy areas and that it is handled at various levels in society. Accordingly, it is interesting to analyse the various perspectives of the government (national security), business and trade policy.

2.2.1 The perspective of government (national security)

As was already, mentioned government has a key role in addressing IT security.

It is possible to argue that information from the public sector has a central role in how the market works and in how an individual may use his/her freedom and rights in society.

The type of information a society can protect and secure is connected to the type of threats versus protective measures that currently exist for that information.

The task for public bodies should be to monitor and identify shortcomings in activities that are critical to society. Technological development, the increasing number of active stakeholders and their interlinkages via global connectivity[47]

have resulted in the need for new approaches and revised regulatory priorities.

There is also a great deal of information that is crucial for society, such as, for example, the management of IT infrastructure for energy and transport. As a result, the view of IT security has expanded beyond a mere focus on technology. Additionally, the approach to IT security is no longer static (avoiding risks); there is also a need for a dynamic approach to risk management, adapting security measures to the constant changes and vulnerabilities in ICT environments.

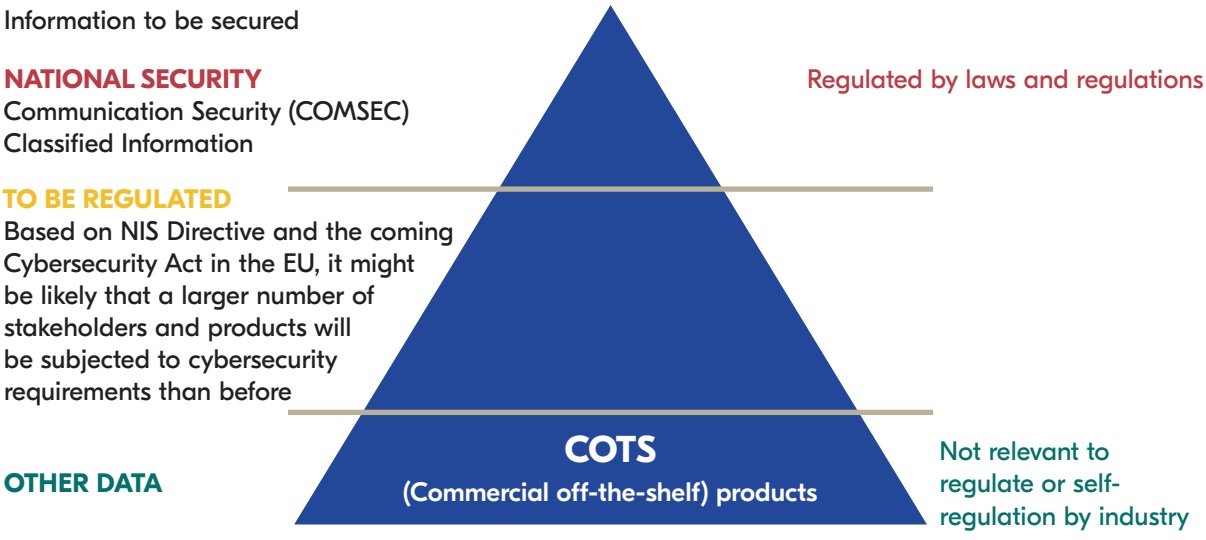
In regard to the regulation of ICT products, it might be useful to use a simplified model to visualise government intervention.

As seen from the illustration, governments have mainly stepped in with regulations within domains that concern national security (defence,

communication security, classified information), which is visualised on the top of the triangle.

For a long time, the triangle was divided only between the top and bottom. With technological development and the advent of new identified vulnerabilities, new incentives have been created for increased governmental intervention. As a

Figure 4. Government intervention in IT security regulation



National security

The concept of national security indicates that government should protect the state and its citizens against all kinds of national crises through a variety of power projections, such as political power, diplomacy, economic power, and military might. Measures taken to ensure national security include (but are not limited to)

- maintaining effective armed forces
- implementing civil defense and emergency preparedness measures (including anti-terrorism legislation)
- ensuring the resilience and redundancy of critical infrastructure
- using intelligence services to detect and defeat or avoid threats and espionage and to protect classified information
- using counterintelligence services or secret police to protect the nation from internal threats.

result, the middle part of the triangle is expanding, which leads to a larger number of ICT products that need to be regulated.

Many commercial ICT products (see lowest level of the tringle) are not covered by technical regulations, i.e., by mandatory government requirements. In practice, the market access of ICT products is facilitated by companies voluntarily applying standards and schemes that provide an attestation of IT security (for a specific market or public procurement). Accordingly, voluntary standards also may become de facto requirements and provide the baseline for business in the sector.

The current regulatory fragmentation manifests itself in how individual countries make their decision regarding what category a product will fall into in the model above.[48] While security agencies and authorities in certain countries require that products be evaluated at the level of national security on the top of the triangle, other countries may be satisfied by lower-level requirements, for example, by requiring a certain evaluation level. As was already mentioned, this approach is dependent on which assets are evaluated as critical or secure from a national point of view (railways, existing infrastructure for mobile networks and so on). The underlying driver can naturally also be to promote national technologies by instituting requirements that keep competing innovations outside the country (i.e., protectionist motives). While few have insight into the differing requirements, it is very difficult to evaluate and compare whether the requirements are in fact effective and relevant.

2.2.2 Business perspective

To seek comments and reflections on the need for greater regulatory harmonisation from a business perspective, DIGITALEUROPE and Swedish Engineering Industries were contacted.[49]

According to those contacts, companies have not expressed any major complaints concerning regulatory fragmentation related to IT security within Europe. Actually, quite a few companies have been reluctant to discuss or share opinions on regulatory fragmentation other than on how IT security regulations and requirements differ in China. There can be multiple reasons for this reaction. Companies might not consider requirements on IT security an obstacle and have adapted to the current regulatory situation. Compliance with mandatory IT security requirements could actually be an issue of competitive advantage. Further, the reluctance to express concerns and information about IT security compliance might stem from the fact that it is a sensitive issue, especially when delivering products and services for critical infrastructure, which might hinder the possibility of disclosing views on the contents of regulatory terms. Regardless, specific product proliferation (i.e., adapting a product for a specific market) is not free, and ultimately, the cost must be borne by the market.

The following compiled comments[50], based on a number of companies, members of DIGITALEUROPE and the Association of Swedish Engineering Industries, are a good reflection of the IT security compliance landscape from a business perspective.[51]

Requirements to comply with and problems with regulatory fragmentation: views expressed by companies

Computer hardware and storage companies confirm that some categories in their product portfolio are affected by IT security regulation, e.g., products for encrypting information flows and data storage, based on EU and national certification schemes (specified as confidential / secret / top secret).[52] On the B2B side, any electronic payment card must qualify for the requirements of the provider, including, for example, certification such as Common Criteria (see Chapter 3).

In the field of public utilities (such as electricity, gas, water), there are applications that companies deliver, such as the protection of critical infrastructures. Compliance is relevant to the NIS Directive (or local regulation, which is basically the transposition of NIS into Member State law). EU regulations on tachographs and the NIS Directive will also become applicable as soon as the technical requirements of clients require it.

Concerning diverging mandatory regulations in various Member States, companies state that in the field of government security there are different schemes based on different national priorities. The companies argue that is not so much an issue of mutual recognition (via Senior Officials Group Information Systems Security SOG-IS mutual recognition agreement MRAs, for example, - see Chapter 3), but it reflects certain national preferences for certain technologies offered by different suppliers. Beyond that (comparably niche) business, the experience highlighted by the companies is that there are not so many differences within Europe regarding sectors such as telecommunications or finance.

The companies explain that the regulatory differences begin with technical specification for products that may carry the same name but have different features.[53] In many cases, regarding public sector driven applications and products, these products may carry the same name in country A and B but have different technical specifications (as the customer has different technical needs, such as in the area of smart metres or health cards). As a result, it is important to be careful when comparing the "same product" between countries.[54]

When analysing regulatory differences outside the EU, companies confirm that there are varying national regulatory systems. The argument is that the significant differences between the U.S., the EU, Japan and China, for example, are not just technical but very political / philosophical. The differences are reflected in decisions on how much technology a supplier should disclose and how useful it is to set up a national industry by fostering national innovation instead of complying with internationally recognised standards.

Companies also confirm that deviating requirements (to a minor extent) can also be found in countries such as Russia (localisation requirements) or India (certain technology testing requirements). Ultimately, from an industry point of view, these measures are not efficient, as they hamper economies of scale.

Companies admit that regulatory fragmentation will always be a cost driver for industry. However, the business representatives argue that the fragmentation needs to be analysed based on sectors (not a cross cutting perspective), as the regulatory outsets between sectors are not comparable. While in areas covered by art 346 TEU and from providers of military equipment,[55] such fragmentation is well known, this reflects a path-dependent development that results, unfortunately, in some markets being blocked for competitive suppliers, depriving (potential) customers of best-in-class technology.[56] For other sectors, such as critical infrastructure, companies expect harmonisation based on the NIS Directive.

Tools for regulatory harmonisation: views expressed by companies

There is an understanding among businesses concerning the intention to harmonise IT security within the EU, referring to the proposal on the European Cybersecurity Act (see Chapter 4.3.1). The Cybersecurity Act aims to reduce regulatory fragmentation in Europe by providing harmonised schemes for IT security certification. However, companies have not historically seen efficiencies in shifting the competencies from the national to the EU level. It is also noted that the IT security industry in the EU has been largely concentrated in France, Germany, Italy, the Netherlands, Spain and United Kingdom.[57] These are the suppliers mainly asking for certification, which is why harmonisation will only help to increase the strength of the European tech industry in IT security to a limited extent. Companies explain the rationale as follows. Harmonisation in the field IT

security is a positive issue in regard to economies of scale. The precondition would be that administrative practices would be the same (having the same standard across Europe) and would create a level playing field (which is not necessarily the case today). Introducing labelling schemes (EU trust labels), which are discussed within the EU Cybersecurity Act, have been received with moderate excitement from companies, as these will not necessarily be a decisive buyer's criterion given the large number of labels that already exist. As a result, it will take a while to build upon the educated buyer that explicitly will ask for certain technology (that may be certified).

Additionally, companies argue that the EU might partially miss the fact that it is the national authorities that ultimately define technical specifications and certification requirements. The authorities therefore have a stronger role in actual market harmonisation than certification schemes alone.

The companies admit that there is room for improvement with regard to the harmonisation of practices (e.g., authority attributes and seeking a certain assurance level (see Chapter 3) according to a standard). Regarding national security exceptions, as outlined in art 346 TEU (crypto mainly), the respondents do not see a clear legal basis for raising certification standards up to the European level. From an international perspective, the companies think that it is vital that new European schemes are accepted internationally, especially to make it easier for SMEs that have already invested in national certification processes.

The businesses further argue that clear B2B topics are mainly driven by sectoral regulation (banking, insurance) or de facto industry standards (automotive as an example). Overall, these national or local requirements can be burdensome for very small, local technology suppliers. However, the more complex technology becomes the more urgent will be the pressure for best-in-class (internationally compatible) technology, which, in turn, will make it more attractive for bigger players to enter these markets. Therefore, evaluations of barriers are difficult to make and are context-sensitive (i.e., not representative in general).

2.2.3 Trade policy perspective

Focusing on trade policy, it can be stated that the approach to the regulation of industrial goods is equal to the promotion of free trade and the improvement of market access for goods across national borders.

Technical regulation under the WTO TBT framework

Three types of product requirements are relevant when analysing technical barriers to trade. These requirements are also an integral part of the TBT Agreement:

Technical regulations refer to mandatory legal documents drafted, adopted and implemented by public authorities that define specific characteristics that a product should have, such as its size, shape, design, labelling, marking, packaging, functionality or performance.

Standards are documents approved by a recognised body that provides rules, guidelines or characteristics for products or related processes and production methods for common and repeated use. Compliance is not mandatory. Standards may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements, as they apply to a product, process or production method. Standards are developed in joint ventures by various stakeholders. The development of a standard can in a number of areas be requested by a regulator. If a standard is made mandatory by legislation, it gains in practice the status of a technical regulation. Standards can be divided into formal standards and other standards. Formal standards are developed by recognised bodies, which should live up to the specific criteria of transparency, openness, impartiality and consensus, effectiveness and relevance. Examples of other standards are de facto standards that are developed, e.g., with a specific sector/area or for a specific company.

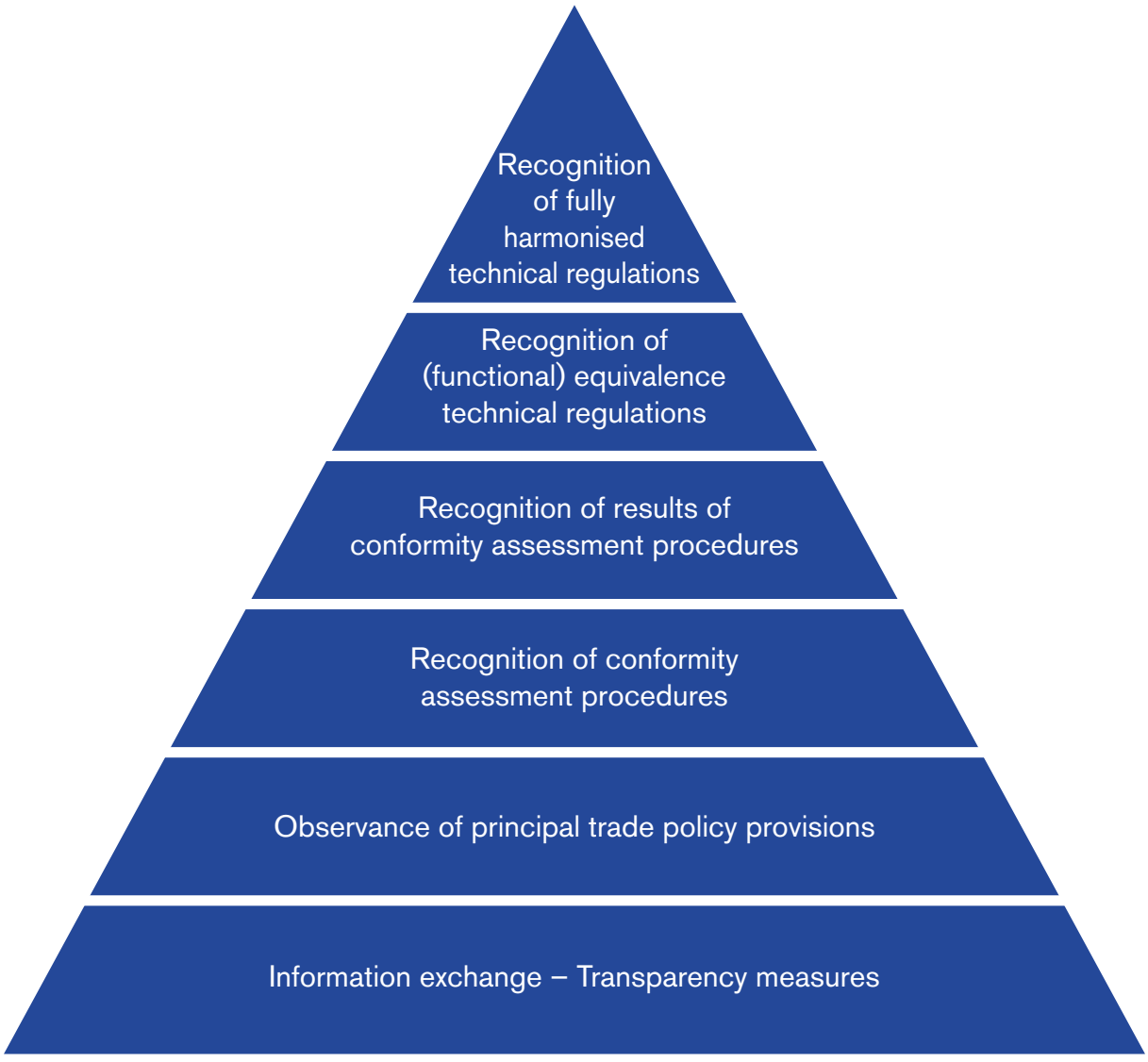
Conformity assessment procedures (CAP)
Conformity assessment procedures are specific procedures used to assess whether a product complies with product requirements. CAP can include, for example, testing, inspection and certification procedures. These can, when hampering international trade, also be covered by the definition of the TBT.

The key mechanism within trade policy that highlights the rights and obligations to regulate is the TBT Agreement under the WTO. The agreement provides the principles that WTO member governments need to adopt and adhere to in order not to discriminate and create unnecessary barriers to trade.

To avoid TBTs for industrial goods, in general, WTO members should use the least trade restrictive measure when regulating goods. The principles in the WTO TBT Agreement enforce the principles of openness, transparency and non-discrimination when regulating industrial goods. WTO members are also supposed to prepare, adopt and implement performance based technical regulations and, as far as possible, the use of international standards and schemes for conformity assessment when regulating. Regarding conformity assessment (testing and certification), the TBT Agreement further highlights the importance of equivalence and mutual recognition based international schemes for conformity assessment. The TBT Agreement, however, recognises individual countries' rights to regulate based on legitimate policy objectives, such as health, safety, environment and, of specific relevance here, national security.

In practice, various countries and regions incorporate various mechanisms to enhance the regulatory convergence among them based on the abovementioned principles. The measures used vary depending on the level of the regulatory ambition sought, as is exemplified by the Regulatory Hierarchy Pyramid.[58]

Figure 5. Regulatory Hierarchy Pyramid



International regulatory cooperation (IRC) may, at the lowest level, simply concern transparency measures in the form of information exchange or, at highest level, may involve full harmonisation of technical regulations.

Somewhat simplified, it could be argued that for many industrial goods there is a basis for international harmonisation, either through international standards developed by recognised standard developing organisations (SDOs) or through international schemes for conformity assessment. These regulatory measures recognise product-specific characteristics, risks and, in many cases, regulatory interdependencies (links between regulatory frameworks). For example, regulating a toy means regulating the chemical, electrical and physical properties in a toy. Although regulators in various countries could argue about the exact level of safety for a toy, the paths to address the regulatory problem are rather uncomplicated because many regulatory alternatives, such as established and widely recognised international standards and schemes for conformity assessment, are available for the regulator. Further, IRC is facilitated by various fora where interested parties may participate, exchange information and have their say.

What concerns IT security in ICT the situation is rather different. The regulatory objective for IT security regulation from the very start is to address national security and societal needs in the widest sense, without a specific need to consider trade.

It is thus understandable that the various regulatory paths that have been developed in the past to address IT security regulation stem from and are based on national needs and concerns to protect critical infrastructure, rather than a strong interest in free trade and international harmonisation. What has changed recently, however, is that the various domains where IT security is vital increasingly embrace sectors and branches which are, from a regulatory point of view, difficult to separate from critical infrastructure. The specific regulatory solutions needed might differ highly depending on the risks a specific product area represents. These premises can make it extremely burdensome to find internationally accepted, standardised regulatory principles and solutions for international IT security regulation. Thus, it is worth analysing which governmental policies and regulatory frameworks are available for the securing information in ICT products.

An evolving perspective that is rapidly gaining recognition and that is relevant in the context of a more holistic view on IT security is that of cyber resilience.

The concept essentially brings the areas of IT security, business continuity and (organisational) resilience together.[59] Although the concept does not solve the problem of how to set or harmonise IT security regulations for ICT products specifically, the concept is valuable in highlighting the interdependencies[60] to be taken into account in policy making concerning IT security regulations. There is a need to accept and create an improved understanding of the connections between national security and trade policy.

3 Technical regulation: a starting point for enhanced regulatory harmonisation

As was already mentioned, there are several ways to address IT security by legislative initiatives. In this chapter, the discussion is narrowed down to one path, namely, technical regulation, i.e., requirements set on ICT products with security features and by conformity assessment[61] such as cybersecurity certification[62] of these products. The reason for the approach is, as was already mentioned, that such requirements have to increasingly become a subject of discussion at the TBT Committee in the WTO.[63]

Cybersecurity evaluation is about formal third-party assessments to determine that products and processes comply with security requirements or standards.[64]

3.1 Common Criteria: the international standard for cybersecurity certification of products

The international standard that provides the technical platform for cybersecurity certification is called Common Criteria (CC).[65] Presenting the CC in this context is important because the standard is used as the basis for government driven certification schemes[66] and because certifications are typically conducted for the use of public agencies and critical[67] infrastructure.

Origins of cybersecurity certification

The origins of requirements for cybersecurity certification, like for most regulations, stem from military standardisation. The basis for cybersecurity standardisation was already established in the 1980s by the so-called Orange Book in the U.S. The Orange Book is also called the Trusted Computer System Evaluation Criteria (TCSEC), which is a standard of the U.S. Department of Defence.

The development of this standard in the U.S. had an impact on Europe, and requirements for cyber security certification were developed, e.g., in Germany and the UK. In the EU, the work with cybersecurity was boosted by the ITSEC Cybersecurity Evaluation Criteria in the 1990s, providing systematic criteria for evaluating cybersecurity in products and systems. The ITSEC is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in those respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the Commission of the European Communities for operational use within evaluation and certification schemes.

Since the launch of the ITSEC, a number of other European countries have agreed to recognise the validity of ITSEC evaluations. When the ITSEC was established, the European Mutual Recognition Agreement on IT security Evaluation Certificates (SOG-IS MRA) was also established as a framework (see 3.1.1 below).

Common international standards and recognition schemes were created later when the ITSEC and the Orange book were compiled.

Certification

Certification refers to the confirmation of that a certain organisation, product or person fulfil the requirements according to a standard or other document. In the field of IT security, the certification process often entails the acceptance of an evaluation.

CC is used as the basis for evaluating the security properties of ICT products and systems, including encryption.[68] The standard allows the specifier, for example, a public authority making a procurement or a regulator, to decide what type of evaluation should be carried out. The standard involves seven different levels for evaluation. These levels are called Evaluation Assurance Levels (hereafter EAL-levels).[69]

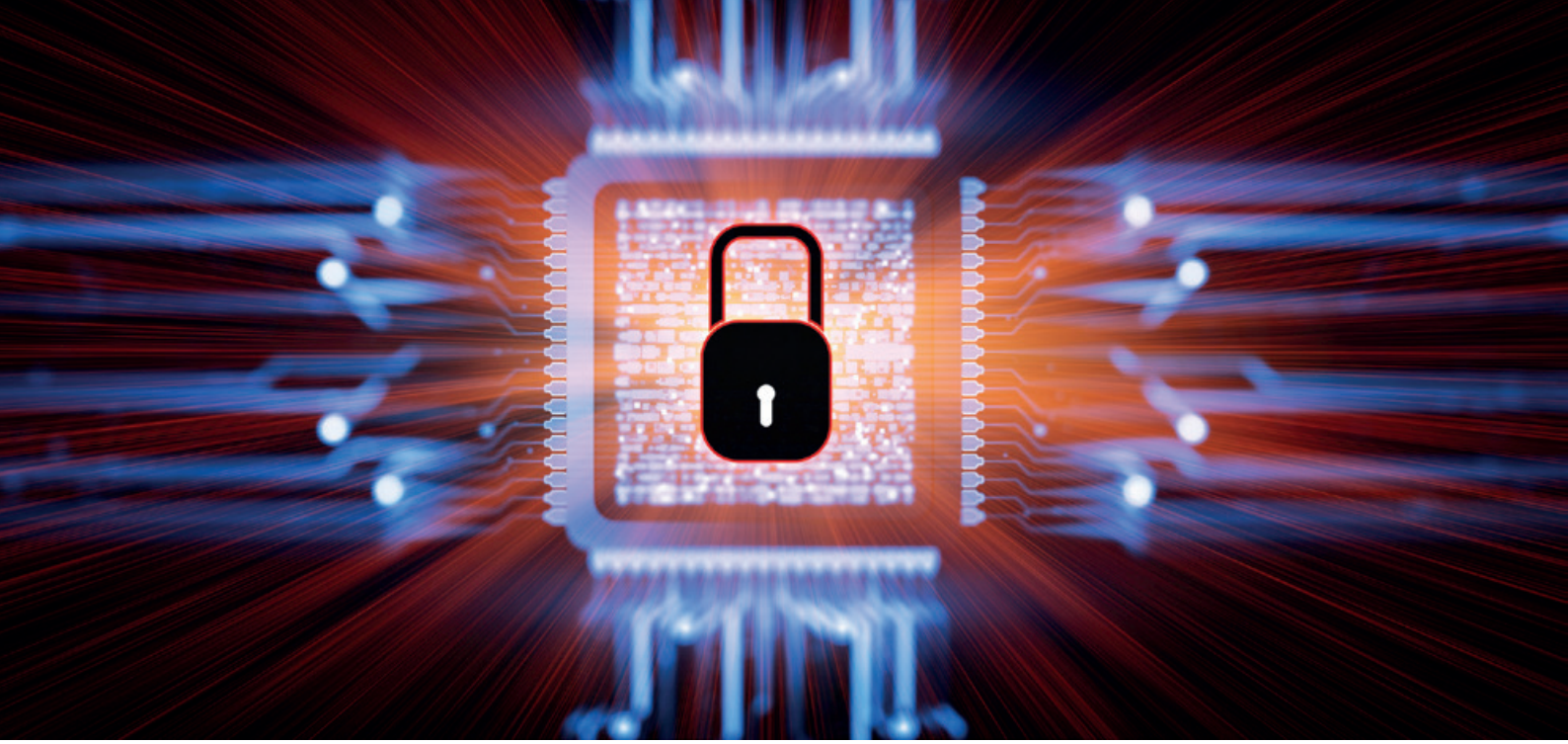
The standard itself does not specify what type of assessment should be carried out; this is left to the specifier (for example, the regulatory body) setting the requirements.[70] The standard is supported by CEM (Common Methodology for Information Technology Security Evaluation), which describes how the evaluation should be carried out, using the criteria and evaluation evidence defined in the standard. Although CEM is part of the standard, it is too generic and is often regarded as quite obtuse.

To create trust and to enable opportunities to ensure that assessments are made in an equivalent manner, so called Protection Profiles (PP) and Supporting Documents are used and are adapted to specific technical areas (categories of ICT products).

PP are documents used as part of the certification process according to ISO/IEC 15408 and the CC. Collaborative Protection Profiles (cPP) following the standard are developed in international Technical Committees (iTCs); this process follows international principles of openness and transparency in standardisation.

Supporting Documents have been developed both on the regional (SOG-IS MRA) and international (CCRA) level for specific product types, i.e., additional requirements for specific product types and technologies. What should be observed, however, is that the development of Supporting Documents does not (compared to PP) always occur through an open process. However, Supporting Documents are still mandatory to use in many cases in order for a supplier to obtain a certificate.

Greater consensus about the practical implementation of the international CC standard through common guidance is naturally beneficial from a trade point of view, i.e., as long as many countries share the methodology and apply the guidance documents in the same manner. It is evident that not all requirement levels in cyber evaluations are prepared, adopted and implemented in full transparency, which risks fragmentation and extra costs for businesses.



3.1.1 Systems for mutual acceptance of conformity assessment (EU/internationally)

Although CC is an international standard that provide a base for conformity assessment and represents an important element in creating regulatory harmonisation for IT security; it very quickly became apparent that a standard alone does not suffice. Systems for the mutual acceptance of other's certifications are needed in order to create greater consensus, trust and acceptance internationally. Accordingly, two arrangements, one in Europe and one internationally, have been developed as follows.

Europe: SOG-IS and SOG-IS MRA

The SOG-IS was formed in response to the EU Council decision[71] in the area of information systems security. The role of SOG-IS is to coordinate European work related to IT security. The work by this expert group resulted in the first version of the European security criteria, ITSEC, published by France, the Netherlands, Germany and the UK. The adoption of the criteria was a success and made it possible to create mutual recognition of certificates among the signatories of the SOG-IS MRA.

The participating members, currently 15 Member States[72] work together to coordinate the development of CC PP and certification policies among European certification bodies.[73] So far, only a few PPs have been developed, such as for digital signatures, digital tachographs and smart cards.

The voluntary Arrangement on the Recognition of CC Certificates in the field of IT, i.e., the SOG-IS MRA in Europe, was initially signed in 1998.[74] Participation in the SOG-IS MRA is restricted to the EU and EFTA states. Currently, there exists cooperation with non-EU countries, such as Turkey and Japan, but the agreement does not recognise certification outside EU/EFTA.

International coordination: CCRA

In the 1990s, IT security requirements needed to be reformed. In 1996, the first version of the CC standard (see 3.1) was published. The conditions for the mutual recognition of cyber evaluations were set by the Common Criteria Recognition Arrangement (CCRA) signed in 1998. The signatories of the CCRA, currently 28 countries,[75] share the common objectives in the area of CCbased evaluations of ICT products. The arrangement aims to ensure the quality of the evaluation of ICT products and PP and contributes to the confidence in the security of these measures internationally. Other goals of the CCRA are to increase the availability of evaluated products, to eliminate duplicate evaluations and to increase the efficiency and cost effectiveness of security evaluations and certification and validation processes of products and PPs.

Comparison of SOG-IS MRA and CCRA

As there is coordination both on the regional (EU) level and on the international (CCRA) level the question is whether there are any differences between the arrangements, principles and practices of the SOG-IS MRA and the CCRA, which

both target the coordination and harmonisation of cybersecurity evaluations?

The main differences between these two arrangements lie in the level of transparency as well as in the evaluation principles used. The SOG-IS MRA, though it is a European arrangement, does not cover all Member States, nor is it an integral part of the EU acquis.

The SOG-IS MRA provides a larger amount of freedom for the evaluators and focuses on the development of requirements for higher assurance levels (EAL4 and above). Within two technical domains, smart cards and security boxes, the SOG-IS MRA has however developed requirements that are more wide-ranging.

The SOG-IS MRA certificates tend to have market value,[76] as certificates often represent a more comprehensive evaluation.[77]

Within the CCRA, essential security requirements are defined for all product types. The development of PPs and Supporting Documents are made transparent by iTCs where countries openly discuss the result. It can be argued that the arrangement highlights a methodology where evaluation should be adapted to be effective and relevant for the market and where the regulation more closely follows the trade friendly principles highlighting openness and transparency.

Regional and international arrangement: effects on the market and security

In comparing the two arrangements, SOG-IS MRA and CCRA, what are the implications of the differences to the market?

From the perspective of trade policy, clear, uniform, harmonised and open standards are always preferable. Due to national security concerns, individual countries do not necessarily share the structures and practices that will be used for cyber evaluation. Consequently, it has been difficult to generate more uniform regulatory schemes for IT security certification internationally, which are normally applied for common industrial goods, such as machinery, electrical equipment or toys, that most countries could adhere to completely.[78]

In general, certification according to the CC is an expensive and lengthy process.[79] The higher assurance levels (EAL) presented by the standard are very easily accepted by the market and do create a demand for more evaluation among suppliers competing with each other. A higher assurance level (EAL) does not, however, necessarily result in a more secure product. This could, but need not, imply a waste of resources. Tailoring regulatory requirements to regulatory objectives seem like a more appropriate path to for advancement.

It could be argued that the two systems, SOG-IS MRA and CCRA, provide for different levels of insight and transparency as well as different possibilities for various countries to participate and affect regulation.[80] Naturally, multiple systems also provide for price differentiation.

From the perspective of trade, it would be important to get assurance that requirements that are prepared, adopted and applied are in fact necessary, effective and relevant for addressing possible risks and vulnerabilities. For less critical product areas, such assurance is easier to obtain. A good reference point here are the essential requirements, standards and conformity assessment procedures applied in the EU for harmonised product areas such as electrical appliances, toys, and recreational craft. In these sectors, product requirements are streamlined and follow a systematic approach to technical regulation. In the field of IT security, a similar analysis is much more burdensome due to variations in what economies regard as critical, and therefore, the ICT environment and vulnerability scenarios change constantly. To evaluate the output from the two existing systems for IT security evaluation (SOG-IS MRA and CCRA) is extremely difficult. Such an evaluation would require insight into the systems and a more comprehensive understanding about the practical implementation and eventual deviations related to "essential requirements" in the field.

3.2 Product-specific technical regulation on IT security: a more complex story

In addition to how ICT products with security features should be certified (evaluated), the existence of mandatory[81] product-specific technical regulations adopted by public bodies is also interesting in this context.

As was mentioned earlier, harmonised mandatory product-specific technical requirements on IT security are relatively scarce.[82] For a long time,

Figure 6. Cyber regulation in the EU[91]

Council decision in the field of security of information systems (1992)

- *provides the basis for the work of SOG-IS with the task to provide advice to the Commission*
- *provides the basis for voluntary mutual recognition of IT security certificates (SOG-IS MRA)*
- *provides a basis for a committee led by the Commission that Member States. The committee has not been active in many years; instead, the certification bodies that signed the MRA meet regularly to work on harmonisation efforts.*

European Network and Information Security Agency (ENISA) (2004)

- *establishes a focal point of expertise and competence in the field of cyber security with the objective of enhancing the possibility for the Members States incl. businesses capacities to prevent and solve problems related to net and information security*

Cybersecurity strategy of the European Union (2013)

- *achieving cyber resilience*
- *drastically reducing cyber crime*
- *developing cyber defence policy and capabilities related to the Common Security and Defence Policy*
- *developing the industrial and technological resources for cyber security*
- *establishing a coherent international cyberspace policy for the EU and promoting core EU values*
- *supporting the development of security standards and assisting with EU-wide voluntary certification schemes in the areas of cloud computing while taking into account data protection, particularly in critical sectors (energy, transport).*

Regulation on tachographs in road transport (2014)

- *lays down provisions concerning the construction, installation, use and testing of tachographs*

Regulation on electronic identification and trust services for electronic transactions in the internal market: eIDAS (2014)

- *eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market.*
- *eIDAS regulates electronic signatures, electronic transactions, involved bodies and their embedding processes to provide a safe way for users to conduct business online, such as electronic fund transfers or transactions with public services. Both the signatory and recipient have access to a higher level of convenience and security. Instead of relying on traditional methods, such as mail, facsimile service, or appearing in person to submit paper-based documents, entities may now perform transactions across borders, e.g., using "1-Click" technology.*
- *eIDAS encourages Member States to use certified solutions to ensure an environment of trust for e-identification, but it does not impose a particular standard.*

General Data Protection Regulation (GDPR) (2016)

- *GDPR provides for a far-reaching framework intended to strengthen and unify data protection for individuals within the EU. GDPR also addresses the export of personal data outside the EU.*
- *The primary objectives of the GDPR are to give back to citizens control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.*
- *The principles and practices presented by regulation foresees cybersecurity and also provides a mechanism for conformity assessment with accredited certification bodies to be used as an element to demonstrate compliance with the requirements.*

The NIS Directive (2016) is the main instrument supporting Europe's cyber resilience. The aim of the directive is to achieve a high common standard of network and information security across all EU Member States. The NIS Directive sets a range of network and information security requirements that apply to operators of essential services and digital service providers (DSPs).

- *The directive highlights some specific sectors (energy, transport, banking, finance, healthcare, drinking water and digital infrastructure).*
- *The directive boosts the overall level of cybersecurity in the EU by ensuring Member States preparedness by requiring them to be appropriately equipped, e.g., via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority to deal with serious risks and incidents that affect the Internet and information systems.*
- *The directive requires setting up a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States. Such an approach, which refers to operational responsibilities and criteria rather than technical product requirements, makes it possible to create effective security without national requirements and inspections that risk creating barriers to trade.*

Proposal for a regulation on ENISA and on ICT cybersecurity certification ("Cybersecurity Act") (2017)

The objective of the proposal under negotiation is to establish a European Cyber Security Certification Framework. The rational is to provide a framework for the development of certification schemes, to prepare standards and criteria for certification schemes, and, by these means, to generate free movement of ICT products and services with security features

these regulations were mostly limited to areas covered by national security.

The existing legal framework in the EU has instead focused on infrastructure. Some product-specific Community legislation can be found for example in the field of tachographs[83] and digital signatures (eIDAS).[84] The regulation on tachographs requires, for example, that certificates of conformity on type approval must be issued by bodies designated by Member States to the Commission. eIDAS regulation encourages Member States to use certified solutions to ensure an environment of trust for e-identification.[85] Other product areas where IT security is essential but where EU regulation does not exist due to national regulatory needs are, for example, cash registers and reporting centres for taxi meters. On one hand, this approach is positive; detailed mandatory technical regulations[86] and standards,[87] possibly deviating from international ones, easily result in fragmentation and market access barriers.

An interesting question in the context is then whether requirements on products and their certification, discussed above, are effective for reaching the main regulatory objective, i.e., IT security.

Specialists argue that even the most comprehensive security evaluation of a product and encryption evaluation might miss the target.[88] It becomes, thus, increasingly evident that a focus on securing products and their certification through regulation needs to be complemented with a focus on securing overall IT infrastructure by combining protective measures.[89] It is already possible to grasp this regulatory approach by looking at the structures within the EU.

The EU targets the achievement of a common high level of security and the establishment of cooperation between member states and operators. The EU Cybersecurity Strategy provides for a horizontal legal framework with a focus on some areas, but it does not have very detailed product regulation. To be more explicit, it is possible to find, for example, requirements on incident reporting and network and information security, which apply to operators of essential services and digital service providers, but direct product regulation is still extremely limited. This situation might change in the short run as the NIS Directive[90] might result in more sector-specific requirements, and the Cybersecurity Act in particular might touch more closely on certain product categories.

In addition to horizontal legal security frameworks, requirements are also part of sector-specific laws, for example, related to telecommunications[103] and privacy.[104] These are not, however, further elaborated upon in this report.

A comprehensive analysis of the regulation of the IT security of ICT products worldwide is beyond the scope of this report. On the other hand, the existing international standards and schemes presented earlier (CC, SOG-IS MRA and CCRA) establish a framework that individual countries need to adapt to if they wish to participate in regional and international systems that provide for harmonisation and mutual recognition in the area.

Based on comments from, for example, representatives of the Swedish telecommunications

industry,[105] instruments such as the NIS and the U.S. Cybersecurity Framework should be promoted. In these frameworks, there are no technical product requirements, but references are made to voluntary standards. The argument is that this approach makes it possible to address security without creating unnecessary barriers. It is necessary to highlight that these frameworks, which are based on voluntary standards, do not automatically make product-specific regulation unnecessary, nor do these frameworks exclude the possibility that the regulator will require stricter requirements in certain areas, which is often the case and, as we can observe, results in regulatory fragmentation.

Below is an attempt to summarise the IT security regulations covering national security and trade policy, highlighting the sources of TBTs.[106]

From a trade perspective, it is possible to compare technical regulation of IT security on three policy levels: national, regional and international.

TBTs

Technical barriers to trade may occur when individual countries are not part of regional or international arrangements, when national, non-transparent technical regulations or requirements on conformity assessment are prepared (without consensus in closed communities and with a lack of will (intentional /unintentional) to avoid duplicating requirements, or when individual countries introduce add-ons reflected in national requirements that differ from international requirements.

Examples:

- Having different policies /view on the cybersecurity certification to be carried out on ICT products
- Using national cryptographic standards
- Requiring in-country testing and the disclosure of source code

BUSINESSES

Individual companies may use a multitude of standards addressing IT security concerns.
These standards may embrace product requirements and requirements for certification that are either general or product/branch specific. Depending on the product, these standards may be required when delivering solutions in the critical sector, to comply with legislation in a certain market, to follow guidelines and to comply with procurement requirements. Companies may apply standards just to address market demand on information security (safety proliferation).

Figure 7. Regulation of IT security in ICT products: Policy approaches at the national, regional and international levels

NATIONAL	REGIONAL	INTERNATIONAL
		
Individual countries may impose national requirements on products to be used in critical infrastructure	Individual countries implement IT security regulations based on regional commitments	Individual countries may implement international commitments related to information security

National level

Regulation at the national level implies that the regulator applies requirements based on its own needs, which basically target risks and vulnerabilities based on threats and vulnerabilities related to national security in the widest sense. Good examples of this approach are mandatory technical regulations related to, for example, cash registers, the energy supply chain, train signalling systems and freshwater supply chains.

Trade Impact

National regulation will always be allowed, for example, for critical infrastructure. The consequence of a lack of harmonisation in other areas might create trade barriers as well as result in unnecessary or inefficient regulation when international standards and/or systems for conformity assessment are not applied.

Regional level

Regulation at the regional level implies that an individual country adheres to and applies IT security requirements based on regional commitments, for example, when EU Member States implement the regulation on tachographs in road transport or take advantage of the mutual recognition of conformity assessment in the field of cybersecurity evaluation (SOG-IS MRA).

Trade Impact

Regional harmonisation creates the possibility of improving trade conditions if all countries in the region share the regional regulatory principles and may affect the regulatory process. If there is a possibility for national deviations or if the regional approach is not compatible with international standards and schemes, there is a great risk for barriers towards third countries.

International level

Regulation at the international level implies that an individual country may implement international commitments related to information security. Examples of this approach are countries that apply the same international standard (CC) for cybersecurity certification or make use of mutual recognition of conformity assessment in the field of cybersecurity evaluation (CCRA).

Trade Impact

International regulatory policies are most likely to promote good trade conditions. The effectiveness of regulatory measures and practices, however, is dependent on how generic or specific the regulatory measures are in order to address a regulatory problem. A voluntary international standard might not solve the regulatory challenge of fragmentation if it is applied differently in different countries. As a result, often, other measures than product regulation are needed. In the case of IT security, for example, authorities could work on requirements for the infrastructure where products are to be used.

4 Regulatory alternatives

What are the pros and cons of regulating IT security? The answers do not so much lie in whether to regulate in the first place but in what to regulate and in what manner (or at which level, product, certification and/or infrastructure).

In this chapter, the focus is drawn to the trade effects of various regulatory paths (regional/international) as well as the possible methodologies in addressing IT security by regulation. The discussion will start with the definition of good regulation and the reasons for a growing number of national, rather than international, IT security regulations. Thereafter, the regulatory landscape in the EU and beyond is discussed in order to follow up with a critical analysis of the main regulatory alternatives (i.e., requirements on certification and on infrastructure) to predict paths forward.

From the perspective of trade and trade policy, a good regulation, in general, is relevant, transparent, non-discriminatory and, to the highest degree possible, based on international standards in order to promote the flow of goods across borders without creating unnecessary barriers to trade.[107] As the analysis in this report demonstrates, IT security regulation has objectives that do not necessarily go hand in hand with trade considerations. Instead, the overarching goal is to protect assets (often national) from threats (often international). As IT security regulation often targets commercial ICT products used in critical infrastructure, the aspects of trade, IRC and regulatory coherence are also becoming more interesting.

Currently, it is possible to conclude that IRC concerning cybersecurity certification is, on one hand, driven by the regional setting within the EU (SOG-IS MRA) and, on the other hand, driven by the international setting (CCRA). While the critical infrastructure becomes more vulnerable and susceptible to attacks, individual countries are increasingly taking the initiative to develop their own standards in the area. This development is driven by several factors. First, it is quicker to develop standards in a smaller group of regional stakeholders than internationally. Second, countries are reluctant to disseminate expert knowledge to stakeholders outside their own sphere regarding how the products are ecured.[108] By developing their own standards, it is possible for countries to tailor the requirements to the needs of the products in their own industry. Naturally, a lack of trust in stakeholders outside their own security domain may contribute to national approaches.

The consequences of this development may be that the suppliers that operate worldwide must follow the development of standards in many regions and certify the security features of their products each time they launch the product in a market. This approach constitutes a barrier particularly for SMEs that might have difficulties conforming outside their own region. Suppliers need to use significant resources for conformity assessment according to regional requirements. The combined expertise of various countries is thus not effectively used, which may risk an inferior and more costly result than if there was cooperation on a global solution. A severely fragmented IT security landscape, established by nations to protect themselves, may thus result in

less secure products and services. Each vendor will need to spend a significant amount of resources and money in certifying their products against a multitude of overlapping national cybersecurity standards. These resources would otherwise possibly be spent on improving the security of the products in the first place.

Finally, there is an obvious risk of TBTs. As regulation and standard setting is accomplished in national or closed communities, there is a lack of transparency and a lack of influence on standard setting by various stakeholders.

Therefore, where do main global actors stand on regulating IT security today, and does any consensus exist on the requirements for commercial ICT products globally?[109] Another important question is also whether the available international standards, such as the CC, are sufficient for proving product conformity or whether additional, national requirements are actually needed to secure the information in ICT products with security features.

4.1 Ongoing regulatory initiatives at the EU level

In general, the required level of conformity assessment for different commercial applications is set by the market. Today, EU IT security certification is based on international standards and the mutual recognition of these with arrangements, such as the CCRA or SOG-IS MRA. However, national evaluation/assessment criteria on different security levels are not transparent (publicly available) nor harmonised among all EU Member States.[110]

The EU regulatory framework presented earlier, concerning the security of products, does not follow the ordinary system for technical harmonisation of industrial goods;[111] instead, it provides at least three different ways of regulating that may include conformity assessment (and mutual recognition thereof):

1. by accreditation[112] (reference to the accreditation requirement is made in the GDPR),
2. Member States may themselves decide on the national certification body (this approach is used in eIDAS), and
3. the European Commission designates certification for the Member State body (this system is used in the field of tachograph regulations).

Additionally, European regulatory areas increasingly rely on CC certification of products, such as e-signature, e-tachograph, e-driving licence, e-ID-card, ehealth care card, and SEPA (banking), making mutual recognition more relevant. As a result ENISA[113], Member States, European Commission and industry players are looking into the possibilities of a lightweight certification or 'security label' for ICT products (see 4.3.1). However, it is commonly acknowledged that this process will take time to accomplish. The question is whether the categorisation and streamlining of required conformity assessment criteria in Europe could benefit from the approach used in

other product areas based on whether requirements go hand in hand with the risks that are identified (from self-assessment at lower levels to rigorous third-party conformity assessment at highest levels). In the absence of an EU-wide cybersecurity certification scheme, it can be concluded that companies have to be certified in each country (except within SOG-IS) and that the EU adopts legislation with different approaches to security certification, adding to the fragmentation of the Digital Single Market.

4.2 IT security regulation internationally

To provide some reference point, below some information and reflections concerning regulation outside the EU are presented.

The United States

The U.S. is developing industry standards to improve security for critical infrastructure and to share information on incidents to strengthen responses. In addition, specific standards are being developed for public authorities, and IT security is to be found in sector-specific legislation.[114]

The national legal framework enables the collection and sharing of information about risks and incidents within the public and private sectors.[115] Further, intrusion and assessment plans must be implemented for federal authorities.[116] In addition, the U.S. Office of Management and Budget (OMB), in its annual reporting instructions, mandates that U.S. federal agencies must use National Institute for Standards and Technology (NIST) computer security standards as well as guidelines, including the field of encryption.[117]

NIST develops industry-based standards and practices for critical infrastructure used by the private sector.[118] Private operators are encouraged to share information (with other operators and the government) about attacks while maintaining confidentiality, privilege, and immunity from liability and anti-trust laws. In other words, NIST's standards and guidelines are mandatory only for U.S. federal computer systems. NIST's standards are not mandatory for U.S. state or local governments or the private sector. The regulations do not address a number of industries, such as Internet service providers (ISP) and software companies. Furthermore, the regulations do not specify what security measures must be implemented; they require only a reasonable level of security. However, sector-specific legislation is to be found, for example, for financial institutions[119] and the healthcare industry.[120]

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a United States Government programme administered by the National Information Assurance Partnership (NIAP)[121] to evaluate the security functionality of information technology in conformance with the CC international standard. As described before, PPs and standards are used to certify products under the CC scheme.

China

Beyond the transatlantic region, China in particular has taken steps that are more radical, and not only technology but also the processes of evaluating IT security are heavily regulated.[122] Therefore, China has more far-reaching policies than other countries in regard to regulations on how IT products can be manufactured, sold and used in the country and to what extent certain product categories must have China as their country of origin. Chinese regulations are the most tangible example of IT security regulation affecting trade and being discussed within the WTO.[123] The concerns that foreign companies have frequently raised concern cases where China has requested the source code in order to certify products and allow export to China. This approach is regarded as a strong infringement on IPR, as the deposition of source code contains the core technology and business. In Europe, in particular, the smart card industry has been affected. The fact that Chinas is not part of the international CCRA means that China is able to sell ICT products worldwide but may impose restrictions on its domestic market that lead to an imbalance in trade. Although both governments and business are eager to highlight Chinese trade barriers in the field of IT security as highly trade restrictive and discriminatory, one should be aware that the Chinese regulatory system in relation to its political context, differs radically from for example of European countries. As a result, without taking a stance on the legitimacy of the regulations, it must be noted that the measures instituted by China are not necessarily fully comparable to measures instituted by other nations.

International cooperation

International cooperation between major economies in the field of IT security do exist as well. Ongoing dialogues that are worth mentioning are those within the GAMS (Governments and Authorities Meeting on Semiconductors), where China, Taiwan, Japan, Korea, the EU and its Member States, and the U.S. participate in developing policies for the regulation of commercial cryptographic products, discussions regarding the Transatlantic Trade and Investment Partnership (TTIP)[124] and the CCRA crypto, where the aim is to create mutual recognition of crypto certification between CCRA members.

4.3 Ways forward?

When looking into the future, one question to analyse is how close or how far apart various countries' approaches to IT security regulation are in reality. In this chapter, some general reflections are first provided regarding the demand for increased harmonisation. Thereafter, the main options or regulatory paths under discussions are presented, i.e., requirements for certification and infrastructure. The chapter will conclude with some remarks on the effects related to both alternatives.

The current regulatory situation in which diverging national regulatory approaches emerge should be a strong motivator for new harmonisation efforts. Harmonisation could improve security but could also address trade, as regulatory harmonisation often creates openness and transparency, which is currently very scarce in the field of IT security regulation.[125] It seems that there is an increasing awareness that there is an urgent need to address security risks in ICT products and that existing systems and structures are insufficient, costly and slow to cover the need for greater assurance to prevent cyber incidents in society. At the same time, there is an understanding that more coordination will be needed, especially to support functioning markets, and that economies need to make joint efforts to identify criteria that can be used by a greater number of stakeholders.

What are the options then for increased regulatory coherence and harmonisation?

In the field of the IT security regulation of ICT products, the two main paths discussed currently are harmonised certification schemes in the EU and national approaches highlighting requirements on ICT infrastructure, as presented in the coming chapters below.

4.3.1 Requirements on certification

The proposal for a regulation for a European Cybersecurity Act[126] is an example of addressing cybersecurity by certification requirements. In the absence of an EU-wide certification scheme presented by the act,

- companies within the EU need to adapt to requirements in each Member States (except within SOG-IS MRA),
- the Digital Single Market remains fragmented,
- the reinforcement of security and users' trust may not be properly achieved, and, most importantly,
- EU legislation adopts different approaches to security certification.

The proposal for the European Cybersecurity Act acknowledges the current regulatory fragmentation in the EU,[127] i.e., that there exist several certification schemes, that several Member States have established national certification systems, and that current schemes result in high costs for suppliers.[128]

The objective of the proposal under negotiation is to establish a European Cyber Security Certification Framework.[129] The rational is to provide a framework for the development of certification schemes, to prepare standards and criteria for certification schemes, and, by this means, to generate the free movement of ICT products and services with security features.[130]

The proposal does not directly address the value of certification in general. The proposal aims to reduce fragmentation by ensuring a common EU-wide approach to certificates recognised in all Member States. One certificate recognised across the whole EU, rather than several for each MS Member State, will provide a significant reduction in cost. The proposal does, however, recognise that a one-size-fits-all approach cannot meet the large variety of needs regarding certification. For example, there are cases where a risk-based approach, which also take into account the operating environment, fully justifies expensive and lengthy certification processes. Other cases do not justify such a process. This difference is

the main driver behind a framework with many "tailored" schemes. Following a risk-based approach will allow the establishment of schemes that are more cost-efficient (cheaper and faster) but are not themselves universally applicable. The schemes are meant to be tailored to the risk. The objective is therefore to improve the overall cost-benefit ratio of certification – not to simply make all certification faster and more inexpensive.[131]

The following European cybersecurity certification schemes that have been suggested for adoption by the Commission include

- specifying a minimum set of elements, including the scope and functioning of the individual scheme;
- specifying the scope and object of cybersecurity certification, including the categories of ICT products and services covered;
- providing detailed specifications for the cybersecurity requirements, for example, with a reference to standards or technical specifications (not only European);
- specifying the specific evaluation criteria and evaluation methods; and
- specifying the intended level of assurance (basic, substantial and high).

The levels initially discussed for an EU certification scheme include self-certification, third-party certification and third-party certification with efficiency assessment. However, the possible coverage sectors and the interdependencies with other Community legislation are only examples of the multitude of aspects that need to be discussed further.[132]

There is no need to question the rationale of the proposal based on the current situation. It is evident that measures are needed to create a more systematic approach to IT security regulation for efficiency, cost and security reasons. The contents of the Cybersecurity Act are also very much in line with the EU system for technical harmonisation and the new approach, although the proposal facilitates greater possibilities for flexibility in adopting schemes that follow various models and standards than in many other areas of goods regulation.

Regarding trade across borders and market access, the voluntary character and international dimension of the Cybersecurity Act could be highlighted and discussed:

The voluntary character of the Cybersecurity Act: Mandatory effects on the market.

- It could be presumed that neither the act (setting up the certification framework) nor the establishment of individual schemes will affect the conditions for market access and the placement of the products and services covered because certification remains voluntary for businesses from EU and third countries, which means that the act itself does not condition market access.[133] Based on this interpretation of the proposal for an act, any ICT product or service available in the EU before the establishment of the schemes would be able to continue under the same conditions as before. For third countries, the schemes should be nondiscriminatory, [134] meaning that vendors/providers from third countries may also apply for certification.

However, with a view to achieving the objectives and avoiding fragmentation, national schemes or procedures for ICT products and services covered by the scheme should cease to produce effects once the date established by the Commission by the means of an implementing act. In addition, it is suggested that Member States will not introduce new national certification schemes providing cybersecurity certification for ICT products and services already covered by an existing EU cybersecurity certification scheme.[135] This means that the act could accomplish harmonisation in the specific product fields agreed upon.

Voluntary schemes could also have the effect of setting a permanent standard for the market, which should be taken into consideration when preparing the schemes under the act. In addition, it should be noted that CCRA already exist to harmonise cybersecurity evaluation among the 14 Member States and third countries.[136] That is, an ICT product certified in Sweden is recognised by India, Korea and Japan and vice versa, which means that suppliers today can rely on one-stop shop certification. If specific conditions for mandatory cyber certification in the EU change, the conditions for mutual recognition between Sweden and, e.g., Japan will no longer be in effect.[137] This situation will double the certification costs both for third-country suppliers that wish to access the EU market within the voluntary framework and for EU suppliers that wish to access the market in Japan.

International dimension: the consequence of the lack of a framework for mutual recognition

- Some Members States (not the EU) are part of the international CCRA. Will their membership will be affected by the establishment of a framework? Based on the proposal, it could be expected that the international dimension will be addressed. As the proposal is open to many schemes, it could be assumed that the Commission and the Member States will ensure that a scheme mirroring the CC will be established to ensure that mutual recognition continues to apply among the CCRA countries.[138]

  The terms and conditions regarding the mutual acceptance/recognition of the certificates of third countries outside the EU have not, however, been specifically addressed in the proposal. Therefore, it is of the utmost importance that new schemes secure compatibility between the existing international and EU schemes. If this is not formalised, for example, through MRAs or other arrangements,[139] the EU schemes will actually create new barriers for third countries. The conclusion here is that the mutual recognition of certificates is as important for addressing fragmentation and avoiding certification costs as for the avoidance of diverging standards.

The proposal is still under negotiation, which makes it difficult to project the exact outcome. The scope and products to be covered by certification schemes have not been confirmed, but the act lists areas where certification is already widely used or is likely to be used, such as automated cars, electronic medical devices, industrial automation control systems and smart grids. In addition, sectors covered by the NIS Directive are mentioned as areas where cybersecurity certification will be critical.

As requirements on cyber certification in the EU today are not harmonised, a central question is whether national security exceptions will be allowed and whether current schemes, such as the SOG-IS MRA, will be compatible with the framework. In this respect, it can be noted that national security falls within the competence of Member States, and the explanatory memorandum in the Cybersecurity Act states that EU intervention does not impede any further national actions in the field of national security matters.[140] How this will be interpreted in practice is however difficult to foresee at this stage.

The act envisages the integration of current frameworks, such as the SOG-IS MRA. Any scheme to be applied under the framework must however meet the principles, requirements and provisions of regulation in the EU Internal Market. The key principles here are transparency and non-discrimination. As these principles should be respected in the preparation and establishment of all schemes, in their subsequent maintenance and in other governance-related activities, it seems probable that this would imply some changes, for example, in the current statutes and operations of the SOG-IS MRA.

The key driver for improved market access is, however, the product and sectorspecific frame-

works to be established under the act. It is too early to predict to what extent Members States will be able to agree on solutions.

4.3.2 Requirements on infrastructure

A complementary approach to addressing IT security is to focus on the infrastructure requirements where products are used. This approach does not create product regulations, such as requirements on certification, unnecessary. Instead, the measures function as a backup that improves security by considering the risks commercial ICT products present from the very beginning.

Again, as presented earlier, increasing vulnerabilities create a demand to evaluate the need for security on the national level as well as for commercial products used to protect data that are classified as sensitive but are not part of national security, for example, in the public sector. An approach focusing on infrastructure is being developed and tested in Sweden.[141] The pilot has been presented to other Nordic countries and has received a positive response. The whole approach targets increasing security by making use of existing certification schemes for ICT products. The logic of the approach is to provide methodological support to regulators, acknowledging the fact that laws and regulations do not provide full coverage for commercial-off-the-shelf products (COTS products).[142]

The pilot focuses on the following:

- Providing security architecture[143] for various types of ICT products. The security architecture works according to a combination principle (for example several layers of crypto) for increased assurance
- Ensuring that the architecture corresponds to the needs of regulatory bodies
- Collaborating with other countries in international fora (iTCs) to ensure a dialogue with developers and to prepare common requirements if possible
- Preparing specifications[144] (cPPs) that provide essential security requirements for products and
- Establishing a website for all interested stakeholders.

From the point of view of international trade, the main benefit is making use of requirements (Protection Profiles) that have been prepared internationally (in ITCs) for a global market without a need to adapt product-specific requirements to national or regional conditions. Therefore, it is possible to prevent the need for several certifications. In addition, a harmonised structure for security architecture with essential technical requirements would make it possible to raise the minimum level security for agencies with security concerns nationally without the necessity to build the competence in each indi-

Infrastructure

An IT infrastructure is composed of physical and virtual resources that support the flow, storage, processing and analysis of data. That is, an infrastructure is the platform used to send data from one point to another.

An example of an unprotected infrastructure is the open public Internet. Examples of a secured infrastructures are the SGSI (Swedish Government Secure Intranet), an intranet separated from Internet for secured and encrypted communication between public agencies in Sweden and Europe, or the TESTA (Trans European Services for Telematics between Administrations) within the EU.

vidual agency, which is currently the case. The recommendation for implementing the solution will probably be based on a user case approach, such as the use case for VPN,[145] so that each agency can implement the security architecture. In this case, the scope is to address internal information sharing needs. Accordingly, the architecture is agency-specific (i.e., not to be shared or used commonly by several agencies).

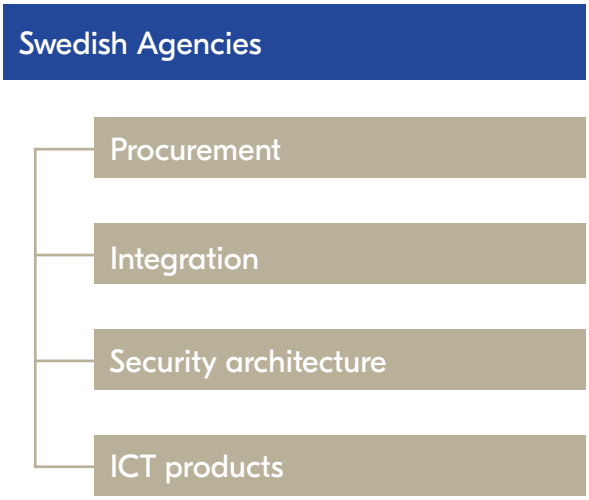
The Swedish pilot programme has been developed bearing in mind that there is a lack of technical regulations or recommendations for security requirements and the use of ICT products with security features that should be secured or are covered by secrecy but that are not part of national security. Further, the IT security for most Swedish critical infrastructure is mainly based on COTS products.[146]

The model is inspired by a system approach established in the U.S. named Commercial Solutions for Classified (CSfC). This approach represents a new way of delivering secure solutions, leveraging industry innovation to quickly deliver industrial application solutions. The approach used in the U.S. has been established to enable commercial products to be used in layered solutions, protecting classified information concerning national security. This approach provides the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

Some possibilities presented by the Swedish pilot programme

The infrastructure solution presented by the Swedish pilot programme targets public authorities. The pilot programme starts from the idea that the solution will be voluntary to use, and no restrictions are made regarding which sectors or stakeholders can apply the infrastructure solution. The programme will provide support and guidance for the development of new infrastructure; however, resources will be needed in order to build and manage the infrastructure in practice, for example, with the support of consultants. The Swedish pilot differs from the approach used in the U.S. since the Swedish approach does not target national security but information that is considered sensitive or has a need to be protected in general. The pilot can be regarded as a downscaled version of the approach used in the U.S.

Figure 8. Building blocks of the Swedish pilot programme for infrastructure architecture



The system approach contains guidance and examples for procuring agencies.

The system specifies and defines the setting for the integration of a refined security architecture that embraces COTS products.

The refined security architecture sets requirements for different IT solutions and specifies the requirements for a secure, layered architecture.

COTS products comply with the pre-set security requirements based on the chosen security architecture.

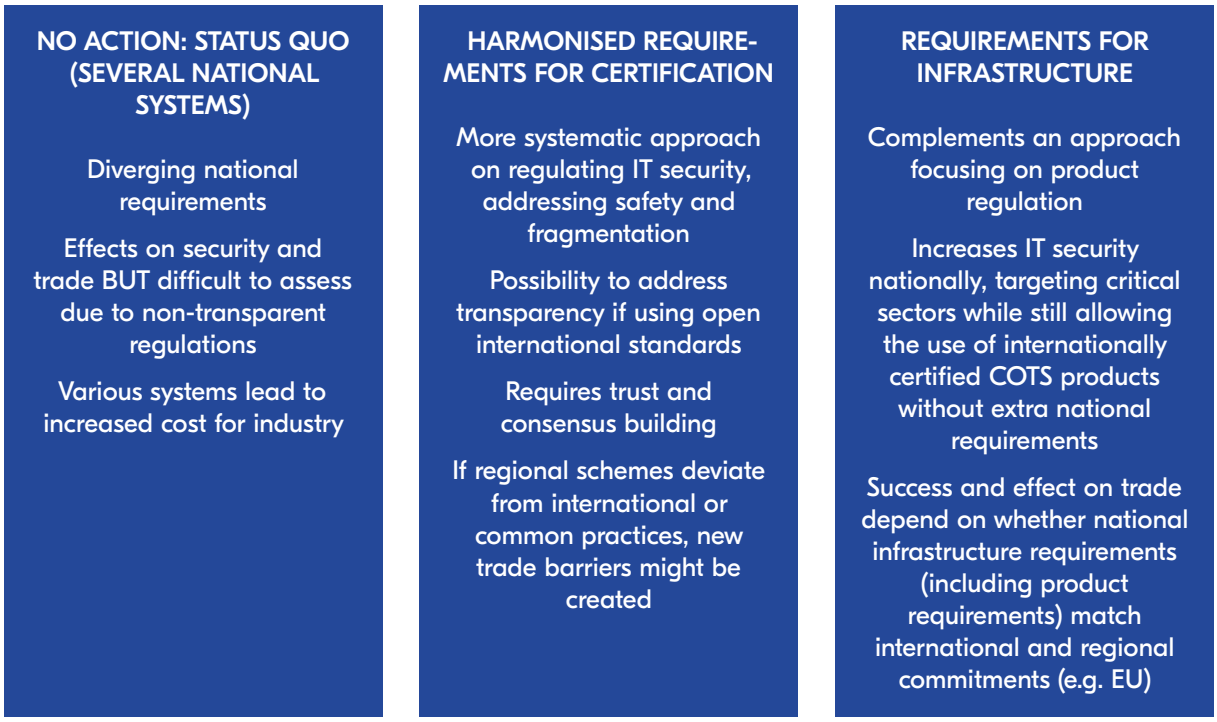
The Swedish pilot is under development, which implies that the details and roadmaps are still to be created for the entire new approach. Similarly, the interconnections between the Swedish system and other proposed systems, for example, in the EU, need to be developed as well.

If the EU framework (the Cybersecurity Act) does not follow international standardisation that allows requirements to be developed with iTCs, it would have a direct impact on the solution (i.e., the possibilities to use fora such as iTCs for developing PP to be used in the solution). This situation would result in the EU framework requiring regional iTCs, with regional requirements, resulting in double the certification procedures (and eventually TBTs).

4.3.3 Effects of different scenarios

To analyse future regulatory alternatives, it might be valuable to compare the impact of the main scenarios for IT security regulation described above.

Figure 9. Regulation of IT security in ICT products- effects of different regulatory scenarios



NO ACTION

Having no requirements on IT security naturally poses serious challenges for both security and trade.

Maintaining the current situation unaltered would imply that individual countries continue to be/not to be part of regional and/or international arrangements, addressing information security mainly by international standards for cybersecurity certification. Eventually, this situation would lead to diverging national requirements in some areas. Whether these requirements contribute to increased security or improved trade (proportionality, time and cost) is difficult to assess, as there is no transparency.

In this regulatory approach, security could constitute a significant problem as there are no harmonised ways to address, evaluate and compare security without insight into the various systems. Taking no action also has an effect on trade, as businesses need to adapt their products to various markets. It is possible that some strict requirements actually are unnecessary or too costly related to the regulatory outcome. Without an insight in the regulations and how the regulations are applied the relevance and effectiveness of measures is extremely difficult to verify.

CERTIFICATION REQUIREMENTS

Applying more uniform cyber certification requirements to a single IT product/component requires the establishment of more structured methodology by which a product gains an acceptable level of conformity. As a certification does not guarantee security, security measures also need to be incorporated into the product development processes. By using open standards and by providing insight into certification, discrimination can addressed. The impact on trade highly depends on how (on which level) the requirements are set (cost profile) and whether these result in mutual recognition and acceptance etween countries.

To prepare, adopt and implement schemes that are suitable for various areas and that many countries agree to might be burdensome. Due to our globally interconnected world, regional frameworks (like the EU) need to take into account interdependencies and use as, far as possible, internationally recognised standards. If new schemes are created, costs could also increase.

This regulatory approach has effects on both trade and security that are dependent on the contents of the requirements and where they are used.

INFRASTRUCTURE REQUIREMENTS[147]

A strategy for regulators could also be to make use of those specifications that are prepared by iTCs and that impose essential requirements on ICT products. Regulators may create a national safety architecture for different types of use cases that correspond to the needs in specific critical sectors, such as transport or health. The focus in this approach is to make use of internationally acceptable requirements for products (e.g., evaluated/certified according to international standards) but to tailor infrastructure requirements to national needs. This approach would create flexibility to adapt requirements for critical systems (such as energy and transport) without affecting market access for ICT products that have undergone an IT security certification (i.e., the regulatory framework is independent from products and suppliers).

As the solution is dependent on suitable architecture, the main concerns might be the possibility of establishing and maintaining the architecture for various domains.

If regional or international regulatory commitments stipulate different binding requirements, it might not be possible to implement this approach on such product areas.

This regulatory approach would have a significantly positive effect on trade and security if infrastructure requirements address and are based on certified (evaluated) products (according to international standards).

4.3.4 Regulatory paths: some policy considerations

In this chapter, the two main paths to addressing IT security for ICT products have been presented: certification requirements and infrastructure requirements. A harmonisation of certification requirements is intended to address IT security on the regional or international levels. Infrastructure requirements are used to address security at the national level, increasing security requirements in sectors that are considered critical. These two paths aimed at improved IT security can thus complement each other.

Whether regulators may take international trade into account when preparing IT security requirements highly depends on which product requirements are used (EU or international), as this choice will affect market access. If two parallel regulatory systems exist (with national and regional requirements, for example), market access for businesses will be hampered.

From a trade point of view, key challenges to harmonising IT security requirements are the perception of security and trust. These are, on a national level, related to critical assets (the information that needs to be protected) and capabilities (the means available to protect the information from attacks,

incidents and vulnerabilities). These parameters are extremely difficult to harmonise, as both the assets and the capabilities are likely to vary to a great extent among different countries.

When policy makers and regulators evaluate policy options for regulatory strategies they should also consider the need for reciprocity and the level of transparency, in addition to the actual regulatory measures. That is, when setting up specific, strict requirements, a nation or region must be willing to accept that other nations will undertake the same regulatory measures. Conversely, it is equally necessary to note that setting up national structures for IT security is closely connected to technical capabilities and policy approaches that might not be comparable and compliant with one's own (critical assets and views on secrecy, censorship, etc.).

As national requirements obviously risk resulting in trade barriers and, eventually, in less secure products, greater harmonisation of requirements would be preferable for actively addressing security, transparency, discrimination and costs by regulation. Where the actual transparency level is set by IT security regulation for specific ICT products, it should probably to be left to the experts in various product areas. Security can be addressed through secure development processes by businesses combined with requirements for conformity assessment (i.e., certification), depending on the product type. As described earlier, regulators should probably refrain from focusing only on the certification of individual products, as certification is extremely burdensome and costly. That is, even if traditional IT product certification schemes deliver value, these have limitations regarding the scalability related to the explosive growth of ICT.

There are opinions that support increased efforts towards making infrastructure requirements mandatory, especially for IT used by public bodies,[148] health care, and banking, i.e., focus-

ing on improved internal control of IT security. This path could be explored further, as the approach can allow market access for commercial products certified according to international standards. This approach also acknowledges the necessity of a public-private partnership, which was often previously neglected, resulting in total reliance on public regulation.[149] To build a specific platform for IT infrastructure, addressing IT security must be naturally motivated based on specific vulnerabilities, as it involves investments. That is, in case the amount of protected information is very limited, it might not be justifiable to develop of a sophisticated IT platform for IT security.

Internationally, the question of trust in relation to critical infrastructure is essential, as some countries pose restrictions on the supply chain, for example, through recommendations not to procure and use equipment from other countries to be used in the critical infrastructure.[150] Additionally, economic sanctions[151] (or threats of them[152]) and enforcement of export control rules can be used by countries as tools to address national security interests.[153] Such measures can manifest as sanctions towards individuals, businesses and governments to address, for example, cyberespionage.[154] It is possible that these challenges cannot be solved by using the existing international trade policy framework due to the national security exception. Nevertheless, it is essential to take trade concerns into account in the context of policymaking.

5 Concluding remarks

A primary question to be addressed in this report was whether the IT security requirements for ICT products may be harmonised to improve trade. An effort has been made to evaluate whether the existing mechanisms within trade policy, such as the principles for the regulation of goods within the WTO, are sufficient to contribute to international harmonisation or whether IT security is and should be a matter of national security policies.[155]

Based on the analysis, it is possible to conclude that IT security in ICT products cannot today be regarded as a harmonised area from a regulatory point of view, although a number of efforts have been made and are underway to enhance regional and international regulatory coherence. IT security is still addressed within national security policies to a high degree. Therefore, the public bodies responsible for critical infrastructure in various countries are the ones that mainly prepare, adopt and apply mandatory requirements on IT security without much concern for market access and trade.[156]

Although there are a multitude of voluntary international standards and schemes for IT security certification, these have not yet been applied by all economies. Nor are the existing international or regional requirements implemented in an open and transparent manner in individual countries, which contributes to regulatory fragmentation. This situation also indicates that existing international trade policy principles and legislative measures are inadequate to contribute to harmonisation and market access in this field, though they may very well address IT security.

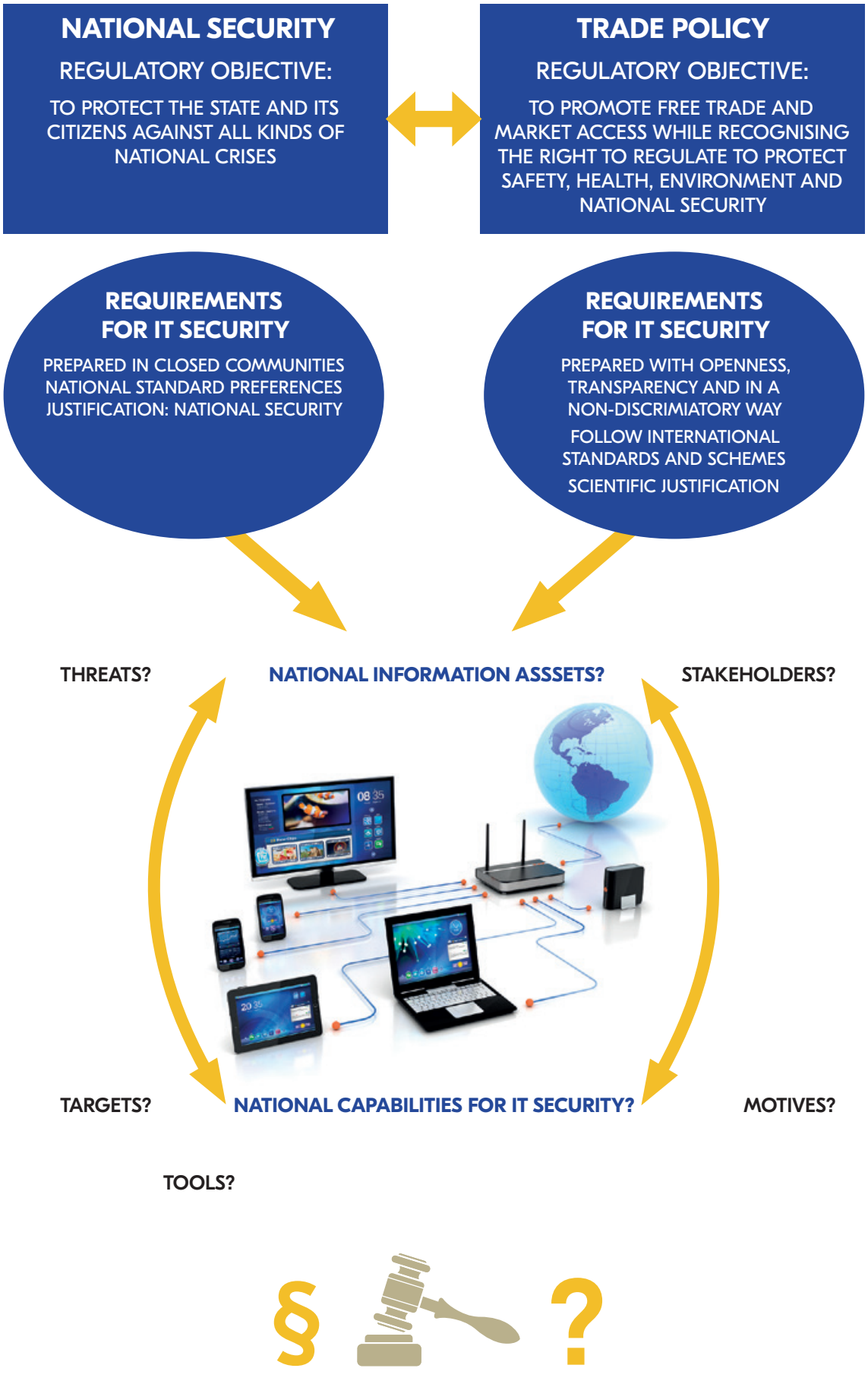
Regarding cyber security certification requirements, an area more deeply evaluated in this report, it is possible to see that although countries make use of available international standards they might still argue for a national security exception in the WTO, though that reasoning does not necessarily motivate the measure or the scientific justification for it.[157] Accordingly, it can be determined that the existing trade policy framework does not provide much support for solving eventual cyber barriers.

Additionally, to date, it cannot clearly be verified that the available standards and schemes for IT security, including mutual recognition, would effectively address regulatory fragmentation worldwide, as TBTs in the field of IT security are increasing.

What is definite, however, is that several new efforts addressing IT security in ICT products are being developed. However, much more analysis needs to be conducted to evaluate the costs and benefits of the various regulatory approaches.

Setting up new requirements and schemes for certification will have major consequences for various industries and for customers and consumers who will pay for the enhanced security. As the comments from businesses reveal, the establishment of new horizontal certification schemes, such as the ones being established through the EU Cybersecurity Act, may not necessarily solve regulatory fragmentation. Therefore, it is crucial that policy makers carefully analyse the consequences of new regulatory initiatives. This approach involves considering the effect these measures will have on security

IT security regulation as a policy challenge



and the manner in which the measures will promote the flow of goods and services while considering global dependencies (the connectivity and transfer of information by various ICT products and services used globally).

One objective of this report has also been to unveil and discuss what the concept IT security entails.

Very often, IT security is regarded as a technical problem to be handled by IT departments, without questioning or analysing the actual threats (confidentiality, availability, integrity), motives (money, power, ideological interests), stakeholders (citizens, societies, nations), targets and tools. Therefore, there is a tremendous need to increase awareness about vulnerabilities related to digitalisation. The level of knowledge must be raised at all levels in society. To address IT security by regulation, it is thus necessary to grasp the consequences for the various stakeholders at the national, regional and international levels.

What is certain, based on this analysis, is that there is a need to continue to closely monitor and evaluate evolving regulatory strategies for IT security. A fragmented IT security landscape, based on national security strategies, may very well ultimately result in less secure products and services.

A conclusion that one can draw from this analysis is that IT security regulation is characterised by a lack of trust. The key will be creating trust among stakeholders and creating trust in the regulatory solutions, as trust is also an essential component for international trade and investments.

Notes

1. For trends in information security see e.g. report of Swedish Contingency Agency, Information security-Trends, 2015.

2. Cyberattacks constitute one of the most significant risks worldwide, both with respect to likelihood and impact. See WEF, The Global Risk Report, 2018

3. National Board of Trade, Protectionism in the 21st century, 2016:2.

4. Each component (i.e. ICT product) within the infrastructure of society may be subjected to attacks. The attacker often faces low costs and small risk of being revealed, while the offence will be difficult to bring to justice. Through the Internet, the attacker has enormous access to critical systems worldwide. (SOU: 2015:23)

5. The main cybercrime players are hacktivists (who are driven by ideology and principles, often to promote transparency, a right to anonymity, human rights and equality, and who use cyberattacks to gain attention), organised crime (individuals or networks who have developed a professional expertise in cybercrime and act for money like profit-maximising enterprises but without moral or ethical concerns) and state-sponsored players (acting directly or indirectly as proxies for national governments, typically military intelligence, to support the geopolitical agenda of their host nation) See Trocmé & Benktander, Cybersecurity, 2018.

6. According to the NATO Co-operative Cyber Defence Center, more than 50 countries/regions have published cybersecurity strategies, including the European Union. See: https://ccdcoe.org/search.html

7. See, e.g., National Board of Trade, Trade Regulation in a 3D Printed World, 2016:1. The responsibilities of various stakeholders (software, printer, person/organisation operating the printer) in relation to the safety and compliance of the product is a complex question. See e.g. National Board of Trade, Online Trade-Offline Rules, 2015:7.

8. TBTs addressed in the Committee for Technical Barriers to Trade within the WTO are called specific trade concerns (STCs).

9. World Trade Organisation Committee for Technical Barriers to Trade.

10. National security refers to the concept that a government should protect the state and its citizens against all kinds of national crises through a variety of power projections, such as political power, diplomacy, economic power, and military might. Measures taken to ensure national security include ensuring the resilience and redundancy of critical infrastructure and using intelligence services to detect and defeat or avoid threats and espionage and to protect classified information. Several definitions of national security exist depending on the context.

11. In practice, the primary objective of new regulatory initiatives is to ensure the functionality of goods and services as well as to secure information. Depending on the regulatory approach chosen, however, the regulations might result in barriers to international trade.

12. According to the TBT Agreement, WTO members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. Therefore, technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks that non-fulfilment would create. Such legitimate objectives are, inter alia, national security requirements; the prevention of deceptive practices; and protection of human health or safety, animal or plant life or health, or the environment. In assessing such risks, relevant elements of consideration are, inter alia, available scientific and technical information related to processing technology or intended end-uses of products (Art 2, TBT Agreement).

13. See for example: Shin-yi Peng, Journal of International Economic Law, 2015, 18, 449-478; Ahrens, National Security and China's Cybersecurity Standards, CSIS, November 2012

14. As recommended by the International Telecommunication Union (ITU), cybersecurity is a matter of national policy because the illicit use of cyber space could hamper economic, public health and national security activities (ITU, National Cybersecurity Guide, http://www.itu.int/cybersecurity/). The question of whether cybersecurity could be regarded as an essential security interest (GATT Article XXI(b)(iii)) is dependent on who has to prove the lack of reasonableness. As Shin-yi Peng (2015) states, "Given the weak restraint on the behaviour of the WTO members under self-judging national exceptions, there is a need for a WTO panel to actively intervene by seeking information from other sources carefully balancing rights and obligations constructed by WTO Agreement and establishing an appropriate trade regime to deal with cybersecurity threats".

15. The new generation of FTAs often have ambitious chapters on TBTs and regulatory cooperation. See for example the FTA between the EU and Canada (CETA).

16. The U.S. has identified 16 sectors that constitute the critical infrastructure, which generally correspond to the areas pointed out in the NIS Directive in the European Union: https://www.dhs.gov/critical-infrastructure-sectors

17. See also Clemente, Cyber Security and Global Interdependence: What Is Critical? Chatham House- February 2013.

18. For many other industrial goods, this would be regarded as gold plating, but as IT security is characterised by sensitivities, regulatory deviations are easily understood. For example, although the requirements are expressed in terms of ISO 15408 (Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model), different countries have certification bodies with different mandates. This means that the standard (in this case ISO 15408) will be applied differently and requirements made differently based on different Protection Profiles (see chapter 3.1 for clarification)

19. In regulating industrial goods through standards, both the EU (Regulation (EU) 1025/2012) and the WTO (TBT Agreement) legal frameworks refer to are openness, transparency, consensus, voluntary application, independence from special interests and efficiency. When such standards are not available, governments should use conforming standards/specifications that are consistent with the WTO TBTs principles, namely, openness, transparency, non-discrimination, consensus, avoidance of unjustified conflict or duplication with international standards, relevance, impartiality and due process.

20. Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM(2017) 477

21. Many companies have pointed out that not only are requirements on certification problematic but so are requirements to deposit or even inspect software source codes. As the source code is equal in value with the software, these type of requirements are regarded as an infringement of IPR.

22. Here it is important to observe that voluntary schemes and de facto standards used in various branches (e.g. banking) provide the same effect as suppliers that do not have a certificate may not access the market. Similarly, governmental regulations in one area may spill over to branch standards, and although they are free to use, they soon create a practice that is copied and used by all companies in a certain market.

23. The right is also manifested by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

24. See also ENISA, Definition of Cybersecurity- Gaps and overlaps in Standardization, December 2015 and Shin-yi Peng, Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, 18, 449-478

25. In order to address IT security within organisations, a management system approach can be applied. Such an approach can cover everything from physical information management, mantraps, encryption key management, malware detection and ransomware and are thus important for maintaining the confidentiality, integrity and availability of ICT systems and business data.

26. A smart card, chip card, or integrated circuit card (ICC) is any pocket-sized card that has embedded integrated circuits. Smart cards can be contact, contactless, or both. Smart cards can provide personal identification, authentication, data storage, and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within organisations. Smart cards are regulated by the Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market in the EU.

27. In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external networks, such as the Internet.

28. Software is instructions that can be stored and run by hardware. Software is often divided into different categories such as application software (which is software that uses the computer system to perform special functions or provide entertainment functions beyond the basic operation of the computer itself), system software (which directly operates the computer hardware) and malicious software or malware (which is software that is developed to harm and disrupt computers).

29. A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.

30. Computer hardware are the physical parts or components of a computer, such as the monitor, keyboard, computer data storage, graphic card, sound card and motherboard.

31. An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.

32. A tachograph is a device fitted to a vehicle that automatically records its speed and distance together with the driver's activity selected from a choice of modes. The drive mode is activated automatically when the vehicle is in motion, and modern tachograph heads usually default to the other work mode upon coming to rest. Tachographs are regulated in the EU through Regulation (EU) No 165/2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport.

33. Cybersecurity legislation is under development in most countries and is generally scattered over different areas of law. One way to group cybersecurity legislation could be in Domestic law security requirements, Laws protecting national security interest and Legislation related to criminalisation of certain cyber activity (see Wiking Häger & Däckö, Cybersecurity Law Overview, April 2017).

34. This as cybersecurity evaluation most often involve the analysis of cryptographic functions. In practice this means checking that cryptographic functions are correctly implemented and that there are not vulnerabilities that allow breaking the encryption in a manner not foreseen.

35. Currently 48 WTO members out of 164.

36. In response to the European Union's Cybersecurity Strategy, the CSCG has published a White Paper underlining the importance of Cybersecurity standardisation to complete the European Internal Market and to raise the level of cybersecurity in Europe in general.

37. Globally there is a huge number of standards with cybersecurity elements. The IEC Advisory Committee on Information security and data privacy standard development (SD) initiative has, for example, identified more than 650 standards and standards developing organisations involved in cybersecurity standardisation, See David Hanlon, Generic methodology for a systems approach for conformity assessment for cybersecurity as the basis for a UNCRO guidelines. Twenty-seventh Session of the Working Party on Regulatory Cooperation and Standardization Policies (WP.6), 30 November 2017.

38. It must be noted that challenges related to information security regulation especially for SMEs are not only limited to mandatory product requirements but also to lack of knowledge of standards, a lack of available capacities, to shortage of standards in specific areas and to implementation aspects.

39. Examples of recent debates related to (Chinese) cybersecurity are regulations that apply to Information and Communication Technology products and concerns, e.g., draft national encryption requirements, cybersecurity review of network products and services, cybersecurity guidelines for vehicles and rules on civil aviation network information security https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm
See also e.g. STCs raised by Canada, the EU, Japan, the U.S. and China concerning India (New Telecommunications related Rules (Department of Telecommunications, No. 842-725/2005-VAS/Vol. III (3 December 2009); No. 10-15/2009-AS-III/193 (18 March 2010); and Nos. 10-15/2009-AS.III/Vol. II/(Pt.)/(25-29) (28 July 2010); Department of Telecommunications, No. 10-15/2009-AS.III/Vol. II/(Pt.)/(30) (28 July 2010) and accompanying template, "Security and Business Continuity Agreement- WTO IMS item 274, India — Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2012- WTO IMS item 367, STC raised by European Union Brazil, Canada, Japan, Korea and the U.S. concerning China (Requirements for information security products, including, inter alia, the Office of State Commercial Cryptography Administration (OSCCA) 1999 Regulation on commercial encryption products and its on-going revision and the Multi-Level Protection Scheme - MLPS)- WTO IMS item 294. Both of these specific trade concerns (STC) have been discussed in the TBT Committee since 2011 and are still on the agenda.

40. Source code means any fully executable description of a software system. See also Glossary

41. Brazil's National Broadband Plan originally included a provision in the public contract for access to source code, China's initial CCC (Compulsory Certification Certificate) required foreign vendors to make their source code available to ensure adequate security, although these proposals were later eliminated. In addition, the Department of Telecommunications (DOT) in India has required foreign equipment vendors to give the Indian government the right to inspect software source code and equipment designs, which has a severe effect on companies' IPR.

42. An example of a requirement for use is a specific national crypto algorithm and protocol.

43. It crucial to note that self-regulation of suppliers by private standards is more the rule than the exception (PCI Security Standards); however, standards not endorsed by governments cannot be addressed formally within the international trade policy framework. ENISA has mapped out the organisations involved in cybersecurity standardisation; see ENISA, Definition of Cybersecurity- Gaps and overlaps in standardisation, V1.0, December 2015.

44. Several reports confirm that cybersecurity legislation is increasing and often springs from national cybersecurity strategies. Not all countries, however, adapt legislation and instead rely on industry standards to set the level of actual security requirements (Wiking Häger & Dackö, Cybersecurity Law Overview, 2017)

45. Several theoretical arguments could be used to explain the need for governmental intervention. Infrastructure providers may lack direct incentives to invest in expensive security measures if they are not held fully accountable for preventable failures. The interdependence between subsystems, components, function-specific equipment and context make it hard to hold any person responsible. Finally, the market partly lacks clear signals about security quality, making it difficult for an interested infrastructure provider to know that their investment was effective. On the other hand, it is obvious that the market invests a great deal in information security and that the driving forces for certification are regulations and recommenda-

tions from public bodies, branch standards/agreements, specific procurement criteria and the market proliferation of suppliers (arguing for safe products).

46. The cost of a cybersecurity certification is more than 50 000-100 000 EUR-, often more.

47. It should be acknowledged that a major part of trade in goods and services is facilitated by data transfers, and most transactions depend on secure communication. All organisations are digital organisations, as operations are dependent on connectivity. See also Clemente, Cyber Security and Global Interdependence, February 2013.

48. Those countries that do regulate to protect their infrastructure get two advantages: their own market is protected from international competition, and by promoting the suppliers in their own country, it is possible to have better knowledge of and say in the products, which means there are fewer vulnerabilities. Accordingly, countries that do not regulate are faced with products from other markets and have difficulties in exporting; additionally, their own infrastructure is built on products from other countries with possible security concerns.

49. DIGITALEUROPE's members include 60 corporate members and 37 national trade associations from across Europe. The Association of Swedish Engineering Industries is an employers' organisation present throughout Sweden and assists 3,900 engineering companies in labour law and industry issues.

50. Views expressed by some of the DIGITALEUROPE and the Association of the Swedish Engineering Industries member's views (anonymously) in January 2018.

51. See also DIGITALEUROPE's position paper on the European Commission's proposal for a European framework for cybersecurity certification scheme for ICT products and services, Brussels, 15 December 2017

52. The companies confirm that for some highly specialised products, such as government encryption devices there is an additional step on top of certification called "admission" which means that products have to be admitted for use in certain contexts.

53. Here the smart meter that has been mentioned in the Cybersecurity Package of the European Commission (see Chapter 4) was provided as an example.

54. The company also highlights the need to observe export regulations that clearly define which product class may be exported to which country.

55. This is limited to non-harmonised areas where there are no secondary laws, and it concerns necessary measures to protect essential security interests in the field of the manufacturing of arms, ammunition and munitions.

56. The companies highlight that national security requirements often call for the maintenance of a national security industry. There is an additional layer on government action where the government acts as an economic entity, and in some cases hold shares in companies and which lead to market distortions to the disadvantage of the private sector.

57. However, countries such as Austria, Denmark, Finland, Poland, Belgium and Sweden have also a considerable share of the cyber market. See CIMA 2018 — Cybersecurity Industry Market Analysis, LSEC & PwC Belgium, March 2018.

58. See for example, National Board of Trade, How TTIP can Address Technical Barriers to Trade, 2015.

59. Entities with a potential need for cyber resilience abilities include, but are not limited to, IT systems, critical infrastructure, business processes, organisations, societies and nation-states. Adverse cyber events are those that negatively affect the availability, integrity or confidentiality of networked IT systems and associated information and services. These events may be intentional (e.g. hacker attack) or unintentional (e.g. failed software update) and caused by humans or nature or a combination thereof. The objective of cyber resilience is to maintain the entity´s ability to deliver the intended outcome continuously at all times, even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms.

60. Today, almost everything (all devices, machines, even vehicles and heath care equipment) is connected to the Internet or to local networks.

61. Conformity assessment procedures (CAP) are specific procedures used to assess whether a product complies with product requirements. CAP can include for example testing, inspection and certification procedures. These requirements, when hampering international trade, can also be covered by the definition of TBTs.

62. The legal framework in the context of the certification of products can be seen on different levels: 1) general requirements as set up by Regulation 765/2008/EC, 2) requirements on the national level from accreditation bodies, 3) certification requirements from various standards and 4) requirements resulting from international arrangements (ENISA, Overview of ICT certification laboratories, Final V.1.1., January 2018).

63. Other regulatory means are legislation on public procurement, which can naturally also contain requirements on products and their certification. Other relevant means are legislation that covers national security and critical infrastructure, which may, but need not necessarily be, relevant to all ICT products with security features sold commercially to both businesses and private consumers. See also Chapter 1.

64. Standards such as ISO 15408 /Common Criteria, ISO 19790, IECEE and FIPS 140-2.

65. It could be claimed that CC is more than just a standard but rather a standardised framework for expressing demands for security in IT products, expressing claims on security provided in IT products (Security Target) and methods and criteria for verifying such claims (assessment of independent 3rd parties). CC has its origins in multiple standards and is the outcome of a series of efforts to

develop criteria for the evaluation of IT security that are broadly useful within the international community. Until 1990, different national origins were apparent. Thereafter, the International Organisation for Standardization (ISO) began its work to develop a set of international standardised evaluation criteria for general use. The current CC standard is identical to ISO/IEC 15408. The current version of the standard is 3.1, Revision 4.

66. Certification according to CC is mandatory in the EU only in some specific fields (such as tachographs) compared with, e.g., the U.S., where the FISMA system is used http://www.nist.gov/itl/csd/soi/fisma.cfm. However, public agencies related to defence have specific criteria for public procurement.

67. Defining critical infrastructure is political and depends on national policies and priorities. In general, it is a term used by governments to describe assets that are essential for the functioning of a society and economy. See Chapter 1.

68. Encryption is, however, scheme dependent and not applicable for all countries.

69. The assessment can be made on different EALs (EAL1 through EAL7). An EAL for an IT product or system is a numerical grade assigned following the completion of a CC security evaluation. The increasing assurance levels reflect added assurance requirements that must be met to achieve CC certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself; it simply states at what level the system was tested. The consignment of source code is required from EAL4-EAL7.

70. The standard is, however, supported by a methodology that describes the minimum actions to be performed by an evaluator in order to conduct a CC evaluation. It could be claimed that the standards provide a range of (seven) various evaluation measures, where EAL 1 represents the lowest level and EAL 7 the most far-reaching requirements. Those who criticise CC argue that the seven levels are too difficult. For certain products, specific evaluations are important, and for other products, the measures at higher evaluation levels are extremely relevant. If EALs are used, one gets much more than is required from the beginning.

71. Decision 92/242/EEC and the subsequent Council recommendation 1995/144/EC on common information technology security evaluation criteria.

72. Austria, Croatia, Estonia, Finland, France, Germany, Italy, the Netherlands, Luxembourg, Norway, Poland, Spain, Sweden and the UK, see www.sogis.org

73. The arrangement provides for member nations to participate in two fundamental ways: as certificate consuming participants and as certificate producers.

74. The original agreement, signed in 1997 (and updated to incorporate the use of CC in 1999), was updated in 2010 for two reasons: to provide a robust mechanism allowing new schemes to take part as certificate producers and to limit the higher levels of recognition to agreed technical domains, where adequate agreement around evaluation methodology, laboratory requirements, attack methods etc. are in place.

75. Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, the Netherlands, New Zealand, Norway, the Republic of Korea, Spain, Sweden, Turkey, the United Kingdom and the United States. Consuming members are Austria, the Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Israel, Pakistan, Qatar and Singapore.

76. The value derives from the assumption in the standard that more evaluation equals with more security.

77. Additional obligations imposed on laboratories are described in the minimum ITSEF Requirements for Security Evaluations of Smart cards and similar device and for Hardware Devices for Security Boxes (Overview of ICT certification laboratories, Final V.1.1., January 2018).

78. Compare, e.g., the streamlined essential requirements, standards and modules on conformity assessment in harmonised (New Approach) directives and regulations in the EU system for technical harmonisation.

79. Within the CCRA, however, certification has become much faster.

80. The statues of CCRA contain explicit requirements that working groups (iTCs) need to adhere to and which follow principles in line with WTO-TBT, See e.g., https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf and https://www.commoncriteriaportal.org/files/communities/Establishing%20iTCs%20and%20cPP%20development%20-%20v0-7.pdf. The rules and the conditions for membership in technical working groups within SOG-IS MRA are defined in JIL subgroup participation rules, See http://www.sogis.org/documents/mra/JIL-SG-rules-v1.0.pdf. Without taking stance on the statues as such, the conditions within the international CCRA seem to highlight more strongly openness and transparency in the operation of working groups, while SOG-IS MRA conditions include limitations with respect to stakeholder participation for both EU and third countries.

81. Naturally, there are a vast number of voluntary practices such as standards and management systems that can be applied to boost cybersecurity in ICT infrastructure; however, such private, voluntary measures cannot be addressed formally within the trade policy framework internationally. Hence, there is a focus on legislative measures by governments.

82. See Figure 6.

83. Regulation (EC) No 165/2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation 561/2006/EC on the harmonisation of certain social legislation relating to road transport.

84. Regulation (EC) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

85. Delegated and implementing acts are in preparation. According to an analysis of ENISA standards, acts

available, in general, address regulatory objectives in the directive, but some gaps still exist (ENISA, Analysis of standards related to Trust Service Providers, Version 1.1., June 2016)

86. A technical regulation is a document which lays out product characteristics or their related processes and production methods, including the applicable administrative provisions, with which compliance is mandatory. It may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements, as they apply to a product, process or production method (WTO/TBT Agreement, Annex 1).

87. A standard is a document approved by a recognised body that provides, for common and repeated use, rules, guidelines or characteristics for products or related processes and production methods, which compliance is not mandatory. A standard may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements, as they apply to a product, process or production method (WTO/TBT Agreement, Annex 1).

88. From a technical perspective, zero risk does not exist in the Internet (O'Harrow et al., Zero Day: the Threat in Cyberspace, 2014). Even when we speak about certification, it can only certify that at this moment, taking into account today's knowledge, the product is secure, which might not be the case the following day.

89. European legislation uses periodic assessments, for example, according to eIDAS regulation, trust service providers (issuers of electronic certificates - CAs) have to undergo an audit every two years (even the European standard requires audits every three years).

90. Some EU acts related to IT security, like the NIS, are directives and therefore require implementation in Member State national laws, which, consequently, entails a certain amount of risk of divergent implementations.

91. The overview in Figure 6 identifies the main legal acts relevant to IT security and demonstrates that, until recently, requirements in the EU have been mainly focused on operational responsibilities and criteria rather technical product requirements.

92. Council Decision (92/242/EEC) in the field of security of information systems.

93. See: http://www.sogis.org/

94. The work of the agency builds on EU initiatives. The agency shall provide advice to the European Parliament and the EU Commission. The agency works, for example, with analysing possible risk, especially at the European level, to contribute to a greater understanding of the Internet and information security to improve cooperation between relevant stakeholders, enhance the development of methods to prevent problems with information security, and contribute to international cooperation (with third countries) (SOU 2015:23, p.182-183).

95. The EU cybersecurity strategy from 2013 embraces protective measures both in the military and in the civil domain.

96. Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. See also Chapter 2.2.3.

97. To be based on ongoing standardisation work of the European Standard Developing Organisations (CEN, CENELEC and ETSI) and the Cybersecurity Coordinating Group (CSCG), the expertise of ENISA, the Commission and other players.

98. Regulation (EC) No165/2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport.

99. Regulation (EC) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

100. Regulation (EC) No 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

101. Directive 2016/1148/EC concerning measures for a high common level of security of network and information systems across the Union.

102. This also requires a network comprising the EU Commission, ENISA, the national incident organisations (CSIRT Network) in the Member States and Computer Emergency Response Team (CERT-EU) for the EU institutions in order to promote swift and effective operational cooperation on specific cybersecurity incidents and the sharing of information about risks; a culture of security across sectors, which is vital for our economy and society, relies heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the States as operators of essential services will have to take appropriate security measures and provide notification of serious incidents to the relevant national authority. Additionally, key digital service providers (search as engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the directive.

103. Directive 2009/140 EC (Telecom Package) requires telecommunications service providers to ensure integrity and provide notification of incidents, for example.

104. EU data privacy rules and the e-privacy directive also require operators to ensure integrity and protect data.

105. Ericsson, March 2017.

106. It must be noted that businesses, especially SMEs may face barriers that have to do with lack of knowledge concerning existing standards, barriers related to capacities and resources, barrier related to shortage of standard in specific areas and e.g. barriers related to lack of implementation guidelines.

107. See principles in the WTO TBT Agreement.

108. Examples include smart cards and NIST curves/algorithms used by FIPS.

109. It is necessary to acknowledge that a great deal of work is naturally conducted by SDOs worldwide to prepare both generic and sector-specific standards on IT security, which are not mapped out nor analysed in this report. In the scope of this analysis, such standards become interesting only when these are referred to in legislation and when they result in barriers to international trade.

110. I.e. although certification schemes seem standardised, they are not, as the requirements of PP and Supporting Documents are not going through an open, consensus-based process like standards.

111. In general, the harmonisation of industrial goods in the EU follows the New Approach. It was conceived in the early eighties and laid down in a 'Council Resolution of 7 May 1985 on a New Approach to technical harmonisation and standards. The approach incorporates the following principles: legislative harmonisation is limited to the adoption, by means of Directives based on Article 100 of the EC Treaty (Rome Treaty, now Art. 95 of the Amsterdam Treaty), of the essential safety requirements with which products put on the market must conform and which will, therefore, enjoy free movement throughout the territory of the European Union (EU); the task of drawing up the technical specifications needed for the production and placement on the market of products conforming to the essential requirements established by the directives, while taking into account the current stage of technology, is entrusted to organisations competent in the standardisation area; these technical specifications are not mandatory and maintain their status of voluntary standards; but at the same time, national authorities are obliged to recognise that products manufactured in conformity with harmonised standards are presumed to conform to the essential requirements established by the directive. This means that the producer has the choice of not manufacturing in conformity with the harmonised standards, but in this case, he has an obligation to prove that his products conform to the essential requirements of the directive. The New Approach also incorporates consistent rules for the testing and inspection of the products according a module structure. See EU Commission: Guide to the implementation of directives based on the new approach and the global approach, 2016 http://bookshop.europa.eu/sv/guide-to-the-implementation-of-directives-based-on-the-new-approach-and-the-global-approach-pbCO2299014/;pgid=GSPefJMEtXBSR0dT6jbGakZD0000fHUZqL7M;sid=F8WjCYhWDTqjCtCgMww9rupzEBal2iqVa5U=?CatalogCategoryID=XwEKABstYp0AAAEjzJAY4e5L

112. In the GDPR, accreditation can mean accreditation by the national accreditation body under the regulation (EC) No 765/2008 or by other government agencies. The purpose of accreditation is to ensure that certification, inspection and testing is high quality and focused on safety for life, health and the environment. Accreditation under regulation (EC) No 765/2008 means that inspections are performed impartially, accurately and based on internationally recognised standards. In some areas, accreditation is mandatory. A company that conducts vehicle inspections or elevator inspections must be accredited. In other areas, such as medical laboratories and calibration laboratories, accreditation is voluntary and serves as a seal of quality. www.swedac.se

113. European Union Agency for Network and Information Security.

114. Wiking Häger & Däckö, Cybersecurity Law Overview, April 2017

115. National Cybersecurity Protection Act of 2014.

116. Federal Cybersecurity Enhancement Act of 2016 and the Federal Information System Modernization Act of 2014 (FISMA)

117. FIPS (Federal Information Processing Standard) certification is required, e.g., for the transport worker ID Card (TWIC), personal identification and verification cards (PIV-Card), and the first responder identification card (FRI-Card). The FIPS is a U.S. government computer security standard used to approve cryptographic modules. FIPS certification is not equivalent to CC evaluation, as the methodologies and the achieved security levels are fundamentally different. ESIA, Draft position paper, 2015.

118. Based on the Federal Cybersecurity Enhancement Act of 2016

119. Gramm-Leach-Biley Act of 1999.

120. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

121. The National Information Assurance Partnership (NIAP) is a United States initiative to meet the security testing needs of both information technology consumers and producers; it is operated by the National Security Agency (NSA) and was originally a joint effort between the NSA and the National Institute of Standards and Technology (NIST).

122. These measures define different levels of protection requirements and are often referred to as the Multi-Layer Protection Scheme or MLPS. Based on the Chinese Cyber Security Law, protection measures through the MLPS include higher standards for protection obligations and closer scrutiny by the government of the operation of critical information infrastructure. Such an approach defines the importance of specific infrastructures and the protections required at different levels. The requirements set by China (China Compulsory Certification) can be regarded as stricter than measures used by other countries. As China is not a member of the CCRA, it is possible for China to sell its own products in other countries and may deny access to the products of other countries, which contributes to an imbalance in trade. See also Ahrens, National Security and China's Information Security Standards, 2012.

123. See e.g. KPMG, Overview of China's Cybersecurity Law, February 2017.

124. The EU negotiation directives on TTIP aimed for greater openness, transparency and convergence in regulatory approaches and requirements and related standards development processes and with the view to adopting relevant international standards as well as, inter alia, to reduce redundant and burdensome testing and certification requirements, promote confidence in respective conformity assessment bodies, and enhance cooperation

on conformity assessment and standardisation issues globally. As an example, ESIA (the European Semiconductor Industry Association), in a 2015 position paper, expressed that wish that no regulation for products with cryptographic capabilities be used in domestic markets as a general rule, except in narrow and justifiable circumstances. The report also expressed the wish for the EU to take a lead in establishing IT security certification policies promoting international standards, the wish for better harmonisation between SOG-IS MRA and CCRA and extended international cooperation, and the wish for more resources for ENISA to work with standardisation bodies and stakeholders to develop technical guidelines and recommendations for the adoption of benchmarks and good practices in the public and private sectors and to define further steps to speed up IT security in the European Digital Single Market as well as in transatlantic ICT infrastructures.

125. Additionally, in other fora, such as UNECE, there are initiatives to map out existing standards and eventual paths for increased international harmonisation. See Hanlon, Generic methodology for a systems approach for conformity assessment for cybersecurity as the basis for UNCRO guidelines. Twenty-seventh Session of the Working Party on Regulatory Cooperation and Standardization Policies (WP.6), 30 November 2017.

126. Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM (2017) 477

127. See the Explanatory Memorandum of the Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") COM(2017) 477), p.6

128. Although there are many examples of regulatory fragmentation, it is not necessarily efficient to point out or compare specific Member States regulations, as the regulatory contexts differ from sector to sector. The automotive industry in Europe has agreed, for example, on a common safety standard for suppliers and service providers using some modules from ISO 27001, which are interpreted independently and combined with custom requirements. Concerning test standards, there are no open standards, and each standard allows only a closed set of examiners.

129. The legal base for the proposal is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which deals with the approximation of laws of the Member States in order to achieve the objectives of Article 26 TFEU, namely, the proper functioning of the Internal Market.

130. See also ENISA, Overview of ICT certification laboratories, January 2018.

131. For some statistics on number of certifications under CCRA/SOG-IS MRA schemes see www.commoncriteriaportal.org. For example in 2015-17, the number of certificates have been 164-221.

132. Commission-ENISA Workshop on Certification and Labelling- Tentative Policy Approaches, Brussels 27 April 2017.

133. As already, mentioned also voluntary schemes may set the standard on the market.

134. See recital 52 in the Cybersecurity Act.

135. The consequences should be evaluated more closely. Depending on the regulatory approach less fragmentation within the EU could at worst case scenario mean more fragmentation between EU and third countries (covered by CCRA).

136. There are 28 signatories to the CCRA.

137. As the application areas of the CC and CCRA are so broad, the introduction of any scheme by the EU risks quickly overlapping with the CCRA.

138. See Art 5 of the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July2, 2014. In practice, however, the EU may need to have an MRA with third country CCRA members.

139. Such agreements are normally negotiated between the EU and third countries in EU harmonised areas.

140. See Art 4 in the TEU and Explanatory memorandum in the proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final, page 15.

141. The Swedish Civil Contingencies Agency is leading the pilot, which involves several national stakeholders.

142. Commercial-off-the-shelf.

143. The security architecture describes each critical component and its security features. ICT products that are included are COTS products that are certified, correctly configured and combined in a manner that ensures that the targeted security is accomplished. The architecture can be modified to meet different needs (different security levels or amounts of information in a system); it is independent of specific IT products and suppliers, and it is layered and combines several components to compensate for insufficient assurance in individual COTS products.

144. That means that the pilot would cover a list of evaluated products according to the specifications (PP that are prepared by iTCs).

145. Virtual Private Network

146. CISCO, Juniper, Microsoft, Apple and Samsung also have a large market share, for example, in Sweden; the utilisation of the infrastructure solution will also benefit end users who will be able to purchase the products more affordably. With the new European certification requirements, it will be more expensive to use these suppliers' products.

147. The architecture will describe each critical component and its security role. The IT products that are embraced are CC certified COTS products that are configured correctly and are combined so that the targeted level of security will be met. See for example https://www.nsa.gov/resources/everyone/csfc/

148. In Sweden, government agencies ought to have a systematic and risk-based approach based on management systems for information security, where the standards ISO/IEC 27001 and ISO/27002 shall be taken into account (MSBFS 2016:1).

149. See e.g. Ewald, SVD Näringsliv, 26 May 2016.

150. https://www.reuters.com/article/us-usa-cybersecurity-espionage/u-s-law-to-restrict-government-purchases-of-chinese-it-equipment-idUSBRE92Q18O20130327, Lee-Makiyama, Stealing Thunder, 2018 and Wiking Häger & Däckö, Cybersecurity Law Overview, April 2017

151. Restrictive measures applied by the EU that are relevance to IT security concern Russia (Regulation (EU) No 833/2014), Korea (EU) 2017/1509 and Iran EU 359/2011.

152. Such threats have been used by the U.S. against China, see https://www.cbsnews.com/news/obama-threatens-sanctions-against-china-over-cyber-hacking/

153. Such tendencies, where nations threaten others and refer to national security in order to pursue trade interests, can already be spotted in the media. These measures reflect decision makers' dialogues rather than established trade policy mechanisms, see for example

154. https://www.pwc.com/us/en/industries/financial-services/regulatory-services/library/sanctions-cyber-crime.html

155. See also Shin-yi Peng, Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, 18, 449-478 for a discussion on information security and cybersecurity related to national security.

156. Due to increasing vulnerabilities and the fact that the use environment of a product is central to its risks and vulnerabilities, it could be anticipated that products will increasingly be regarded as critical for society and, thus, become embraced by regulations that affect market access internationally.

157. This is because the requirements and methods used in the certification process are not open and transparent for all.

References

Literature

Arrangement on the Recognition of Common Criteria Certificates in thefield of Information Technology Security, July 2, 2014.

Ahrens, Nathaniel, *National Security and China's Cybersecurity Standards*, Center for Strategic International Studies, CSIS, November 2012

CIMA 2018 – Cybersecurity Industry Market Analysis, LSEC & PwC Belgium, March 2018

Clemente, David, *Cyber Security and Global Interdependence: What Is Critical?* Chatham House- February 2013

Common Criteria Recognition Arrangement Development Board, Establishing International Technical Communities and Developing Collaborative Protection Profiles, 28 February 2014

DIGITALEUROPE's position paper on the European Commission's proposal for a European framework for cybersecurity certification scheme for ICT products and services, Brussels, 15 December 2017

ESIA- European Semiconductor Industry Association, *Draft position paper- IT Security, Encryption and Certification requirements in the context of the TTIP negotiations,* Brussels, January 2016

EU Commission: *Guide to the implementation of directives based on the new approach and the global approach,* 2016

European Semiconductor Industry Association, *Draft Position Paper, IT Security, Encryption and Certification requirements in the Context of the TTIP Negotiations,* Brussels, January 2015 - Date 12.2.2015

European Union Agency for Network and Information Security (ENISA), *Analysis of standards related to Trust Service Providers,* Version 1.1., June 2016

European Union Agency for Network and Information Security (ENISA), *Annual Incident Reports 2016-Analysis of Article 13a annual incident reports in the telecom sector*, June 2017

European Union Agency for Network and Information Security (ENISA), *Definition of Cybersecurity- Gaps and overlaps in standardization*, V1.0, December 2015

European Union Agency for Network and Information Security (ENISA), ENISA Threat Landscape Report 2017- 15 Top Cyber Threats and Trends, Final version 1.0, ETL 2017, January 2018

European Union Agency for Network and Information Security (ENISA), Information security and privacy standards for SMEs, December 2015

European Union Agency for Network and Information Security (ENISA), *Overview of ICT certification laboratories*, Final V.1.1., January 2018.

Ewald, Fia, *Förnya arbetet att säkra information*, SVD Näringsliv, 26 maj 2016

Friedman, Allan, *Cyber Security and Trade- National Policies, Global and Local Consequences*, Center for Technology Innovation, September 2013

Gunnar Lindström & Heidi Lund, *Common Criteria for Information Security Evaluation - Current Scope and Future Challenges,* European Organisation for Testing and Certification (EOTC) News Letter: In-depth articles, 2003

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

KPMG, *Overview of China's Cybersecurity Law*, IT Advisory KPMG China, February 2017

Lee-Makiyama Hosuk, *Stealing Thunder*, Occasional Paper No.2/18 European Centre for International Political Economy,

Myndigheten för Samhällsskydd och beredskap, *Informationssäkerhet- Trender*, 2015

National Board of Trade, *How TTIP can Address Technical Barriers to Trade*, May 2015

National Board of Trade, *Online Trade-Offline Rules*, 2015:7

National Board of Trade, *Protectionism in the 21st century*, 2016:2

National Board of Trade, *Trade Regulation in a 3D Printed World*, 2016:1

Robert O'Harrow Jr, *Zero Day: the Threat in Cyberspace*, The Washington Post, 2003

Ross J. Anderson. *Why cryptosystems fail.* Commun. ACM 37, 11 (November 1994), 32-40.

Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, Journal of International Economic Law, 2015, 18, 449-478
SOG-IS Recognition Agreement, Management Committee Policies and Procedures, JIL-SG Rules v1.0, February 2012

Statens Offentliga Utredningar, *Informations - och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten* (*Swedish Government Communication, Information and Cybersecurity in Sweden. Strategy and measures for secure information in central government*), SOU 2015:23

Swedish Civil Contingencies Agency, Regulations and Advice on information security for government agencies- MSBFS 2016:1

Trocmé, Johan & Banktander, Ellen, *Cybersecurity*, Nordea Corporate & Investment Banking 03/2108

U.S. National Institute of Standards and Technology (NIST) *Federal Information Processing Standard (FIPS) 140-2 "Security Requirements for Cryptographic Modules" Requirements and Scope,* April 2012.

Verizon, 2017 *Data Breach Investigation Report- 10th Edition*,.

Wiking Häger, Erica & Däckö Carina, *Cybersecurity Law Overview*, Mannerheimer & Swartling, April 2017

World Economic Forum, *The Global Risks Report 2018 13th Edition*, World Economic Forum, Geneva, 2018

Websites

https://ccdcoe.org/search.html

https://censys.io/blog/freak

https://csis-prod.s3.amazonaws.com/s3fspublic/180213_Significant_Cyber_Events_List.pdf?Yrnw.5AEZjDWzNsYnbixw8_6GXMc9YNW

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-andterrorism/critical-infrastructure_en

https://ec.europa.eu/energy/en/topics/markets-and-consumers/smartgrids-and-meters

https://ec.europa.eu/digital-single-market/en/news/communicationcybersecurity-strategy-european-union-%E2%80%93-open-safe-andsecure-cyberspace

https://www.ENISA.europa.eu/news/ENISA-news/white-paper-ondigital-security-published-by-european-standardisation-bodies

https://www.dhs.gov/critical-infrastructure-sectors

http://heartbleed.com/

http://internetofthingsagenda.techtarget.com

http://www.itu.int/cybersecurity/

www.lsec.eu/CIMA

http://www.nist.gov/itl/csd/soi/fisma.cfm

https://www.pwc.com/us/en/industries/financial-services/regulatoryservices/library/sanctions-cyber-crime.html

https://www.reuters.com/article/us-usa-cybersecurity-espionage/u-s-lawto-restrict-government-purchases-of-chinese-it-equipmentidUS-BRE92Q18O20130327

http://www.risidata.com/Database

http://www.sogis.org/

www.swedac.se

https://www.weforum.org/agenda/2016/07/cyber-resilience-what-toknow/

https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm

Glossary

Accreditation
Accreditation is a formal evaluation competence that is based on regional or international standards. Accreditation is a method and a tool to evaluate and approve organisations/bodies that inspect, certify or verify other parties' products, services, plants or systems. Accreditation is carried out by an accreditation body. Accreditation is used in both mandatory and voluntary areas.

Botnet
A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attacks (DoS attacks), steal data, send spam, and allow attackers to access a device and its connections. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a combination of the words "robot" and "network". The term is usually used with a negative or malicious connotation.

Breach
An incident that results in a confirmed disclosure, not just potential exposure, of data to an unauthorised party (compare with **Incident**).

Certification
Certification refers to the confirmation of that a certain organisation, product or person fulfils the requirements of a standard or other document. This confirmation is often provided by some form of external review, education, assessment, or audit on a continuous basis. Often the certificate is valid for a limited time period. Certification is not a protected concept, which might make it difficult to assess the reliability of a certificate. Certification systems can, but do to have to, be operated under the domain of accreditation. In certain domains, it is mandatory to be certified.

Product certification also covers processes and services.

In the case of IT security, the certification process often entails the acceptance of an evaluation.

Cloud
Cloud storage is a model of data storage in which the digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible and the physical environment protected and operating. People and organisations buy or lease storage capacity from the providers to store user, organisation, or application data.

Common Criteria
The international standard that provides the technical platform for cybersecurity evaluation is called Common Criteria (CC). The standard is identical to ISO/IEC15408.

Communication Security
Communication security (COMSEC) is the prevention of unauthorized access to telecommunications traffic, or to any written information that is transmitted or transferred.

Conformity Assessment Procedures (CAP)

Conformity assessment procedures are specific procedures used to assess whether a product complies with product requirements. CAP can include, for example, testing, inspection and certification procedures.

COTS

Commercial-off-the-shelf or commercially available off-the-shelf products refer to hardware or software that can be purchased on the open market, as opposed to developed or specially ordered developed soft or hardware. COTS products are often also called standard programs or standard products.

Critical Infrastructure

Defining critical infrastructure is political and depends on national policies and priorities. In general, critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and an economy.

Cryptography, Cipher Key (see also Encryption)

Cryptography can be described as a discipline, which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. A cipher (or cypher) is an algorithm that transforms meaningful data into seemingly random data, and back again, when needed. Encryption is the act of scrambling the data, and decryption is the act of restoring the data to its original form. To encrypt or decrypt a key is needed. The key is the only part of a cipher that should need to be secret in order for the cipher to be secure (i.e., even if everything else is known about the cipher it should still not be possible to decrypt a text without knowing the key). How strong a cipher is (i.e., how easily it is broken) is usually directly dependent on the length of the key. Applications of cryptography are for example used to protect ATM cards, computer passwords and Internet transactions. Cryptographic means are also frequently used in e-id and electronic signatures. Depending on the proliferation of an individual product and its use area, an incident (for example, Heartbleed, vulnerabilities in a program library OpenSSL and Freak, deficiencies in crypto standards) may seriously affect the users involved and be dangerous from a societal point of view. Even if there are flaws in algorithms and protocols, however, many of the failures in cryptographic systems come from implementation errors (e.g., Heartbleed) or improper use (e.g., Freak) of the system. In economic terms, it could be argued that a cipher key represents the aggregated value of all the information that is protected by it, for example, all bank transactions, the correct status of electricity supply in a given city/country or communication with a ministry.

Cybercrime

Cybercrime, or computer related crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrime may threaten a person's or a nation's security and financial health.

Cyber resilience

Cyber resilience refers to an entity's ability to deliver the intended outcome continuously despite an adverse cyber event, even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms.

Cybersecurity (compare with Information Security)

Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its independent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the

networks and infrastructure and the confidentiality of the information contained therein. In this report, cybersecurity, when used, is not restricted to the protection of (national) information and systems from major (often foreign) cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage; instead, the term embraces the entire area. **In this report, the term IT security is mainly used**.

Cyberspace
Cyberspace refers to the set of links and the relationship among objects that are accessible through a generalised telecommunications network and to the set of objects themselves, where they present interfaces allowing their remote control, remote access to data, or participation in control actions within that cyberspace.

Cyber threat
Cyber threat means any potential circumstance or event that may damage, disrupt or otherwise adversely influence networks and information systems, their users and affected persons.

Denial-of-service attack (DoS attack)
In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. Denial-of-service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-ofservice attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack by simply blocking a single source.

Encryption in IT Security Regulation (see also Cryptography)
Encryption is an important parameter in creating IT security. Cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages.

Firewall
In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external networks, such as the Internet.

Hacker (Ethical Hacker)
In computing, a hacker is any skilled computer expert that uses his/her technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated with a "security hacker", i.e., someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. An ethical hacker is thus an expert that uses his skills to reveal bugs that may allow persons or organisations to threaten IT security.

Hacktivist
Individuals or networks who gain unauthorised access to information to promote social or political ends, often with the objective of engaging the public by drawing attention to a critical cause.

Hardware Security Module (HSM)
A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.

Incident
A security event that compromises the integrity, confidentiality or availability of an information asset (compare with **Breach**).

Information Security (compare with Cybersecurity)
The aim of information security is to protect information so that it will always be available when needed (availability), so the information can be trusted, so that the information is not manipulated or destroyed (integrity), so that only authorised persons may access it, and so that it is possible to follow how and when information has been handled and communicated (traceability). Information security covers administrative (e.g., technical regulations and management systems), technical and physical measures to protect information (such as, e.g.,

physical passage controls and clean desk policies). **In this report, the term IT security is mainly used.**

Internet of Things (IoT)
The Internet of things is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators and network connectivity, which enable these objects to connect and exchange data.

Key management
Key management is the management of cryptographic keys in a cryptosystem. Key management includes dealing with the generation, exchange, storage, use, and replacement of keys. Key management includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Malware
Malware, short for malicious software, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Management system
A management system is the framework of policies, processes and procedures used by an organisation so that it can fulfil all the tasks required to achieve its objectives. Typical areas where management systems are applied and that are based on international standards include quality (e.g., ISO 9000-series), the environment (ISO 14000-series), social responsibility (ISO 26000-series) and information security (ISO/IEC 27000-series).

Mantrap
A mantrap is a physical security access control system comprising a small space with two sets of interlocking doors in which the first set of doors must close before the second set opens. In a manual mantrap, a guard locks and unlocks each door in sequence. An intercom and/or video camera are often used to allow the guard to control the trap from a remote location. In an automatic mantrap, identification may be required for each door, sometimes possibly even different measures for each door. For example, a key may open the first door, but a personal identification number opens the second. Other methods of opening doors include proximity cards or biometric devices, such as fingerprint readers or iris recognition scans.

Mutual Recognition Agreements (MRA)
Mutual recognition agreements (MRAs) promote trade in goods between the European Union and third countries and facilitate market access. MRAs are bilateral agreements and aim to benefit industry by providing easier access to conformity assessment.

National Quality Infrastructure (NQI)
The structures and mechanisms that provide the basis for confirming the safety and quality of products and services in an economy are referred to as the national quality infrastructure of that economy. The main elements of a quality infrastructure are the legal framework, defining the rights and obligations of the institutions and the economic operators involved in quality and safety; the legal framework for law enforcement on the safety of products and services; regulators who issue technical regulations on safety of products; metrology institutions, providing primary measurement standards and traceability; standards institutes, which develop and issue voluntary standards; accreditation bodies for thirdparty attestation of the competence of conformity assessment bodies; conformity assessment on the market and market surveillance authorities, which ensure that the economic operators market products and services that are safe and do not endanger human and animal life and that contribute to a sustainable environment.

National security
National security suggests that governments should protect the state and its citizens against all kinds of national crises through a variety of power projections, such as political power, diplomacy, economic power, and military might. Measures taken to ensure national security include ensuring the resilience and redundancy of critical infrastructure and using intelligence services to detect and defeat or avoid threats and espionage and to protect classified information. Several definitions of national security exist depending on the context.

New Approach
The relationship between standardisation and legislation at the European level has been developed in accordance with the so called New Approach to technical harmonisation and standards, which was introduced in 1985. See, e.g., http://ec.europa.eu/DocsRoom/documents/18027/

Operating system (OS)
An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.

Phishing
Phishing is the attempt to obtain sensitive information, such as usernames, passwords, and credit card details and (money), often for malicious reasons, by pretending to be a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using bait in an attempt to catch a victim. Thus, citizens are the fish, and the villains are trying to get us to "nap" and disclose information in order to gain control of our credit card or bank account data, often by emails.

Pretexting
Pretexting is a form of social engineering in which one individual lies to obtain privileged data about another individual in order to engage in identity theft or corporate espionage.
A pretext is a false motive.

Protection Profiles (PP)/ Collaborative Protection Profiles (cPP)
Protection Profiles (PP) are documents used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC). Requirements for cybersecurity in IT products can be made in the form of PP that follow a standard. PP express the implementation of independent sets of security objectives for a type or category of IT products. PP also specify the security requirements and assurance measures that fulfils those targets. International technical communities (iTCs) are formed to produce and maintain cPPs. In a cPP the organisation setting the requirements prepares (together with other stakeholders) a tailored solution for the specific product type that is described in the cPP.

Ransomware
Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.

Scam baiting
Scam baiting is a form of Internet vigilantism, where the vigilante poses as a potential victim to the scammer in order to waste their time and resources, gather information that will be of use to authorities, and publicly expose the scammer.

Secure development process
Security is part of the software development process, is an ongoing process involving people and practices, and ensures application confidentiality, integrity, and availability. Secure software is the result of security aware software development processes, where security is built in, and thus, software is developed with security in mind at every stage of the software development lifecycle (SDLC).

Secure Enclave
The Secure Enclave is part of the processor (A7) by Apple and newer chips used for Touch ID, which is a fingerprint scanner. The Security Enclave is used in Apple products to secure fingerprint data for better security. Within the Secure Enclave, fingerprint data are stored in an encrypted form which, according to Apple, can only be decrypted by a key available to the Secure Enclave, thus walling off fingerprint data from the rest of the A7 chip and the rest of the iOS. The fingerprint function and the data are stored in a specific part of the processor that cannot be read by the rest of the processor, Apple IO or Apple in general.

Software
Computer software, or simply software, is a part of a computer system that consists of data or computer instructions, in contrast to the physical hardware from which the system is built. In computer science and software engineering, computer software is all the information processed by computer systems, programs and data. Computer software includes computer programs, libraries and related non-executable data, such as online documentation or digital media. Com-

puter hardware and software require each other, and neither can be realistically used on its own.

Source Code

In computing, source code is any collection of computer instructions, possibly with comments, written using a human-readable programming language, usually as plain text. Source code is the set of instructions and statements written by a programmer using a computer programming language. This code is later translated into machine language by a compiler. The translated code is referred to as object code. Programs may contain one or more source code text files, which can be stored on a computer's hard disk or in a database or can be printed in books of code snippets. Source code is the only stage where a programmer can read and modify a computer program. Source code can thus be regarded as intellectual property.

Spyware

Spyware (stalkerware or spouseware) are computer programs installed on a phone or computer in order to spy on the user. If your computer or mobile phone is infected by spyware, your text messages can be read, your calls can be listened to, or your microphone and camera can be activated at any time to listen to you, to gain access to your photos or to track you anywhere worldwide.

Supporting Documents

Supporting documents are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.

Tachograph

A tachograph is a device fitted to a vehicle that automatically records its speed and distance and the driver's activity selected from a choice of modes. The drive mode is activated automatically when the vehicle is in motion, and modern tachograph heads usually default to the other work mode upon coming to rest. The rest and availability modes can be manually selected by the driver while stationary.

Tailgating

Tailgating, sometimes referred to as piggybacking, is a physical security breach in which an unauthorised person follows an authorised individual to enter a secured premise.

Technical Barriers to Trade

Technical requirements on products can in certain circumstances result in unnecessary obstacles to international trade, so called Technical Barriers to Trade (TBTs). The preparation, adoption and implementation of technical requirements are regulated by the WTO Agreement on Technical Barriers to Trade (TBT Agreement). The aim of the TBT Agreement is to ensure that product requirements and procedures used to assess compliance with those requirements do not create unnecessary obstacles to international trade.

Trade policy

Trade policy often refers to governmental measures that a country or group of countries undertake to affect international trade. The means are dependent on the objective and the level of freedom the country has within the agreements it is part of. Trade policy measures can open up or narrow market access (free trade vs. protectionism). The traditional definition of trade policy mainly embraced agreements and requirements for trade in goods. Today, trade policy also concerns regional and multilateral systems, including trade in services, investments, and intellectual property rights (IPR) protection. Therefore, the division between trade policy and other policy areas has become more blurred. Trade policy instruments relevant to the regulation of industrial goods concern Technical Barriers to Trade (TBT).

Virtual Private Network (VPN)

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. ("In the simplest terms, it creates a secure, encrypted connection, which can be thought of as a tunnel, between your computer and a server operated by the VPN service.") Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network

Acronyms and Abbreviations

ACSEC	Advisory Committee on Information Security and Data Privacy
CAP	Conformity Assessment Procedures
CC	Common Criteria
CCC	China Compulsory Certification
CCEVS	Common Criteria Evaluation and ValidationScheme (US)
cPP	Collaborative Protection Profile
CSIRT	Computer Security Incident Response Teams
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT-EU	Computer Emergency Response Team
COMSEC	Communication Security
COTS	Commercial-off-the-shelf
CSCG	Cyber Security Coordination Group
CSfC	Commercial Solutions for Classified
DOT	Department of Telecommunication
DPS	Digital Service Providers
EAL	Evaluation Assurance Level
eIDAS	Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
ENISA	European Union Agency for Network and Information Security
ESIA	European Semiconductor Industry Association
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
FISMA	Federal Cybersecurity Management Act

GAMS	Governments & Authorities Meeting on Semiconductors
GATT	General Agreement on Tariffs and Trade
GPA	Agreement on Government Procurement
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IMS	Information Management System (WTO)
IoT	The Internet of Things (IoT)
IRC	International Regulatory Cooperation
ISO	International Organisation for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
JIL	Joint Interpretation Library (SOG-IS)
MLPS	Multi Lawyer Protection Scheme
NIAP	National Information Assurance Partnership
NIS	Network and Cybersecurity (NIS) Directive
NIST	National Institute of Standards and Technology
NSA	National Security Agency
Orange book	Trusted Computer System Evaluation Criteria, a Computer Security Standard
PCI	PCI Security Council
PP	Protection Profile
SDO	Standards Developing Organisations
SEPA	Single Euro Payments Area
SGSI	Swedish Government Secure Intranet
SOG-IS	Senior Officials Group Information Systems Security
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
STC	Special Trade Concern
TBT	Technical Barriers to Trade
TCSEC	Trusted Computer System Evaluation Criteria
TESTA	Trans European Services for Telematics between Administrations
TTIP	Transatlantic Trade and Investment Partnership
UNCRO	United Nations Confidence Restoration Operation
VoIP	Voice over Internet Protocol (Korean National Standard)
VPN	Virtual Private Network
WAPI	WLAN Authentication and Privacy Infrastructure (Chinese National Standard for Wireless LAN's)
WTO	World Trade Organisation

2018 06

Box 6803, S-113 86 Stockholm, Sweden
Phone +46 8 690 48 00 Fax +46 8 30 67 59
E-mail registrator@kommers.se www.kommers.se