Ladies and Gentlemen,

When we speak of power in military and security terms in the digital world, we invariably recognize that this world itself began in the military research realm. Be it Alan Turing during the Second World War, working on decrypting Enigma or the origins of the web in DARPA, the Defense Advanced Research Projects Agency, we recognize that like with so many technological innovations, the digital world originated in the defense establishment.

Yet it would be a mistake to confuse etiology with contemporary use; just as knowing that NASA sponsored the development of Velcro, does not really come to mind when you fasten your running shoes.

For while all of us here know that the digital world is increasingly a battlefield, where state and non-state actors, nations, criminals and terrorists, sometimes in collusion, or in novel public/private partnerships, use the explosive development of the web for military, espionage and extortion ends, the defense establishment has become the tail of the dog.

Although everything we call "cyber" began with military research, the military side does not occupy the minds of those millions of people involved in all things digital except at conferences like these. Indeed the military as opposed to the criminal side of "cyber" was not taken seriously at all as late as nine years ago, when Estonia was subjected to what is considered the first Clausewitzean continuation of policy by digital means.

Indeed, if you go a mile down the road today to our major annual Startup conference Latitude 59, you will find plenty of young innovators working on the internet of things, smart health and so on, whose thoughts are far removed from the military and defence matters you are discussing.

Not that digital means had not been used before that to achieve political or military ends, but the 2007 massive DDOS attacks on Estonia are considered the first case of an attack by one country against another. Back then, though, we were told not even to think of invoking article 4,

let alone 5 of the North Atlantic Treaty.

Nine years later, on the eve of the Warsaw summit, just as an example of how much attitudes have changed, we anticipate NATO to name "cyber" as the fifth domain of warfare, after Land, Sea, Air and Space. That in some way shows how much thinking has changed in less than a decade.

While I cannot but welcome this understanding that digital means can be just as effective militarily as kinetic means, or more bluntly, that some lines of code can just as effectively knock out a power plant as a missile, I nonetheless believe that we are putting the cart, or in more military terms, the caisson before the horse.

If we look at defense, it is a national prerogative. Cyber-defense, even more so is national prerogative. For while NATO allies strive for the interoperability of kinetic weapons systems, so that a British missile should be mountable under the wing of a French Mirage jet, for example, cyber-defense has no such requirements. But, as I have lamented for years on this stage, when it comes to cyber, we find ourselves rather in intelligence agency mode, where we share as little a possible and only when necessary.

Not that NATO does not share, but not in ways outsiders think. NATO's Co-operative Center of Excellence for Cyber Defense, headquartered here in Tallinn, focuses on research and development of technology and concepts, and on legal issues. NATO's NCIRC only works on NATO's own cyber-defense, that is, defending the organization's own networks. There is no joint NATO cyber capability, still no NATO cyber operations.

NATO's main cyber efforts, however, remain focused on military defense of the organization itself. While recognizing the importance of civilian networks and the risks they face, NATO lacks the legal or policy levers to address these questions directly.

At the supra-national level, the European Union has also begun to deal with cyber security, supplementing or superseding member state policies in a number of areas, including those related to economic, justice, and home affairs. While national governments guard their sovereignty in the areas of defense and foreign policy, the EU maintains some limited authority in these areas. In fact, the EU is developing a considerable role in shaping the European

cyber-security landscape, primarily through legislation and expenditures related to economic regulation, individual rights, and internal security.

So some progress is being made on threats that are supranational. But let us think through, what it is that we are talking about, when we talk about keeping our networks and systems safe. Which systems?

We worry first and foremost about civilian and commercial networks. We worry about power grids and traffic control systems, hospitals; we worry about banks and financial markets, credit cards, personal data records. All of these have come under attack; serious or large-scale damage to these in the digital age can have disastrous consequences for our populations, our economies.

In addition we have IoT, machines talking to machines, chips talking to chips. The worries of the broader public, which focus on issues such as privacy pale, indeed are miniscule, compared to the damage that can be wrought with attacks on data integrity, an issue we all of us need to explain better than we have. And not only to the public but also to our political leaders, parliament members and policy makers, whose understanding of these kinds of threats are, alas, not very sophisticated.

But you all know this, of course. What I would like to draw greater attention to is that almost all the these systems whose security you worry about are commercial products, both software and hardware. Companies, banks, municipal SCADA systems, IoT-based cars and refrigerators, manufacturing processes are all vulnerable. And the more modern, the more digitized, the less legacy-based the system, the more vulnerable.

In other words, we are concerned about commercial software and hardware produced by multinational or international companies; the same Microsoft or SAP or Oracle software and Intel, Alcatel, HP or Huawei hardware is used the world over.

Through the years, I have asked the question of whether the Westphalian state system can still work in a digital 21st century. Historically, our security has been implemented and guaranteed by national-territorial units, also known as states.

Today, however, in the digital world, the digital domain, the most fundamental aspects of our security represent an intimate and inextricable intertwining of the state and the private sector.

The private sector has a different set of concerns. With commercial products security considerations are driven by the bottom line. These companies may have headquarters in Palo Alto, Beijing or Walldorf, but their customers span the globe. So they may care about security, but they need to care about the security of their customers across the world.

So it would be unsurprising to see situations where companies and governments pursuing the same aims ultimately, disagree about how to achieve security. Witness the showdown between Apple and the FBI over unlocking an encrypted iPhone – two actors, opposed to one another, but ultimately committed to security, but with very different visions of how to get there.

Usually we end up talking about PPP, public/private partnerships, government working together with the private sector. Yet as I mentioned, the private sector is multinational and international, privacy, integrity and security concerns are historically strictly national.

So far, when we have seen conflicts between IT companies and territoriality, they have primarily been about taxation, extraterritoriality of jurisdiction as with U.S. government's purview over data in servers abroad.

It is a truism, ladies and gentlemen, that in the world of cyber, geography ceases to play a role, all distances are equal. Unlike conventional warfare, there is, in the case of cyber an equality of threat regardless of distance. All the more so when we overwhelmingly use software and hardware sold and used around the world.

With hard- and software used around the world and territorially based states responsible for security of systems used in those states, we clearly have a problem with suggestions for closer co-operation between the government and private sector.

Unless of course states get together to work with the private sector.

To agree on minimum standards, issue certificates of origin for hardware that these days may contain components of dubious origin despite the good reputation of the final fabricator. Or to issue warnings when one country discovers a zero day exploit, a new worm, etc. That is the kind of thinking we should develop.

Clearly this is difficult, especially when we consider authoritarian and undemocratic regimes. NATO as a group of like-minded and basically value-based nations could serve this function but so far has not, locked, as I mentioned, in espionage rather than interoperability mode. Moreover it is also geographically based, not really useful in in the instantaneous, borderless digital. Where would that leave Australia, Japan, South Korea or Chile? Or even local non-members such as Finland, Sweden and Austria. As the threats that we face know no geography, why should defense?

So perhaps what we should consider is something like John McCain's, and before that Madeleine Albright's "Community of Democracies", ideas floated in the late nineties and first decade of this century. Not NATO but democracies that are concerned about digital security. A club of rule of law based democratic countries that also certify software and hardware, where membership is a privilege that also carries benefits to those who join.

I rush to say this is most decidedly not a grouping like the conventions proposed in various forms often by undemocratic authoritarian countries that involve, inter alia replacing ICANN with the ITU or with treaties that would limit freedom of expression, indeed even allow for censorship on the world wide web.

The democratic and rule-of-law nature of a country would be the primary consideration for membership, something like the Copenhagen Criteria that needed to be fulfilled for countries even to begin being considered for EU accession. Except we would leave out the geographic dimension. All countries, with no geographical limit, could join the digital security organisation.

One such constellation already exists, the Budapest Convention, originally the Council of Europe convention on cybercrime, where signatories obligate themselves to extradite cyber-criminals. We do not need to recall that the primary sources of cyber crime are countries

that have refused to accede to the convention.

Getting this right, of course, will be very difficult and indeed could be considered utopian. With a quarter century in foreign policy, negotiating inter alia Estonia's EU and NATO accession and any number of other agreements, I know full well how difficult it would be to bring together nations, private corporations and get all to agree on something that works, let alone is robust.

Yet something along these lines, I believe, will be necessary if we are to get genuine public-private co-operation to guarantee our citizens and nations security in world where digitization has permeated our lives so completely. And will continue to do so at an accelerating pace, following Moore's Law.

The earlier we start, the less damage we will face.