Today, the opening of the annual CyCon conference in Tallinn marks more than simply the sixth time this gathering has taken place. Last year, the speaker after me was General Keith Alexander. We also met that afternoon right before he flew off. About half an hour after his wheels up, the Guardian broke its story on Edward Snowden. So I am very glad I am not the se cond
speaker here.

Ladies and Gentlemen,

For 7 years I have been trying to convince fellow politicians and leaders to deal with cyber, to convince them that it is a genuine security threat. Or, to be more precise, that developments in digital technology render all of our previous, kinetically based security thinking, certainly not irrelevant witness Eastern Ukraine, but that security threats have extended to every aspect of life that is digital.

People were slow to realize this change. The Munich Security Conference, the West's premier conference on security had its first panel on cyber security as late as 2011, that was three years ago. International Security, the leading journal of security policy published its first article ever on the issue of cyber only last year. Tellingly, the author, Lucas Kello, is Estonian.

Now, however, we have the opposite problem. Everyone sees cyber problems everywhere, even where they do not exist or are highly unlikely. Not that we see much more public attention to defense of our critical digital infrastructure, SCADA systems, our digitized financial system and so on. Rather, because of what became public the afternoon of the first day of last year's CyCon, we have entered a Pynchonian mindset, where we worry that every last corner of our lives is being monitored somewhere by someone. In many innocuous, fundamentally commercial cases – our Google searches, Facebook "likes" – this may even be true, but it feels nonetheless noxious.

The intervening year has forced us to re-evaluate virtually everything we know and think about the cyber world. This re-evaluation has not always produced the most desirable outcomes; at the level of our citizens we have seen a dramatic increase in paranoia about what goes on on the web. In terms of NATO and relations among democracies trans-Atlantic as well as intra-European relationships have suffered enormous damage. Our hopes for cloud computing,

e-services such as e-medicine have suffered as well. We see pushes for an autarkisation and isolation in the call for national webs. Authoritarian regimes are gleeful, democracies frustrated. Freedom online is under threat more than ever.

In other words, the cyber world, something discussed here in the context of defense, active or passive, has become like defense itself, part of the larger world of competition between states, of interstate and economic relations. If before it was a struggle to get cyber to be considered part of defense, cyber has now become an issue of the world at large.

First there is the issue of privacy. Until last year, anyone in the field knew the fragility of privacy online, but the general public did not. Now we see that a priori assumptions among people about lack of privacy are ubiquitous, even when we should know that technologically, say for example in the case of deep packet inspections, the amount of resources required to engage is so great that most people can continue to write and send their innermost private thoughts without worrying about a reader over their shoulder.

Secondly, and more dangerously, because it can affect policy and freedom, one of my concerns in a previous opening speech here, is the specter of a breakdown in the universal, open and borderless internet. Generally people use the term "balkanization" to describe this phenomenon, but I think it is offensive to attribute something pejorative to the Southeast corner of Europe so I prefer the more neutral and I believe more accurate term of the "Westphalianisation" of the internet, based on the 1648 treaty of that name that stipulated that each country can do what it wants within its own borders. Even when not dealing with authoritarian countries that have leapt on the chance to justify isolation and so-called national firewalls, we have seen too many calls by people who should know better to cut their countries off from a U.S. administered internet. Or to regulate the Internet intergovernmentally through an organ of the United Nations, the ITU.

Indeed I just finished chairing ICANN's Panel on Global Internet Cooperation and Governance Mechanisms and we just published our report Towards a Collaborative, Decentralized Internet Governance Ecosystem that makes a series of recommendations on internet administration so that it would not be taken over by an intergovernmental body, but rather would remain open to all stakeholders. It is a battle we thought we had won at the ITU a year and half ago but after the revelations of the past year, the whole issue came roaring back to threaten us again. I am not sure we have won that battle, but the ICANN group came together to make recommendations to preserve the model that we currently use.

Finally, we once again have been reminded after the US Dept of Justice indictments of five Chinese military officers that the use of cybertechniques has allowed a greatest explosion of mercantilism – using the state's apparatus to advance its economic interest – what Adam Smith attacked almost 250 years ago in his classic of liberal economics, The Wealth of Nations. That is, we see cyber is not just the defense of critical information infrastructure, but it is also the basis of economic policy; what used to be called industrial espionage itself now takes place on an industrial scale, if you will, as part of nations' attempts to create a strategic advantage over their competitors, both military and commercial.

So let there be no mistake. The damage done by these revelations, or more accurately and often, their not always judicious journalistic representations, which tend to the simplistic and sensationalist, as well as public perceptions based on these accounts, has been immense.

Ladies and Gentlemen,

If up till last year it was difficult to get policy makers beyond a limited set of cognoscenti interested in cyber, then today we face the opposite problem: getting people in the cyber world to accept the constraints of democratic practice and notions of privacy in the Free World.

Personally, I think much of the problem we face today represents the culmination of a phenomenon, or a trend, diagnosed 55 years ago by C.P. Snow in his essay "The Two Cultures": the absence of dialogue between the scientific-technological and the humanist traditions. Snow was both a respected scientist as well as well-known poet, who noted that he could talk to his colleagues in either realm but the rest of his colleagues in either group did not undersand the other.

Today, this problem of late fifties Oxford faculty clubs permeates our lives. Bereft of understanding of fundamental issues and writings in the development of liberal democracy, fundamental rights and freedoms, computer geeks devise ever better ways to track people... simply because they can, or ... "Isn't this cool, I just figured out how to do X". Humanists – politicians and lawmakers, journalists, lawyers and poets – on the other hand generally do not understand either the underlying technology or math and are convinced, for example, that tracking meta-data means the government reads their emails.

C.P. Snow's two cultures today not only do not talk to each other, they simply act as if the other doesn't exist.

This is not a problem, of course, in illiberal and authoritarian societies where such issues often are taken to be signs of decadence and weakness. The atomization of knowledge and the social sphere indeed supports authoritarian regimes. The point, however, is that if we are to foster the development of a digital world that is open and free, we must develop and follow certain rules. Rules understood by the creators of technology and technology understood by those whose concerns are fundamental rights and freedoms.

One way of doing this is actually to study more math, especially among humanists.

And one attempt to lay down the ground rules, as I mentioned, is ICANN's document on maintaining a multi-stakeholder model of Internet governance. Another is the Netmundial, which must be taken as the response of the international community, and especially civil society, to the Snowden revelations. A third is the Freedom Online Coalition, established three years ago and chaired by Estonia this year, of liberal democracies pledged to uphold internet freedoms and an open web. In short, we need to work toward and reach agreements on the norms of behavior regarding the cyber world and develop adequate defenses against those that do not accept the norms of openness and freedom.

Let me also offer the dystopian alternative, that in part is already with us. We can become autarkic and protectionist as we choose to use systems from our own country, or in the case of the EU, only from members. I am not making this up – such suggestions have actually been made. We can go the way of the defense industry – that is, expensive bespoke solutions, opaque deals between government and industry, and cross-border trade that includes healthy doses of lobbying and bribery. Do we want to take all the industries that have flowered massively, and throw it down the drain? To have the power industry, the car industry, the router industry look like the defense industry? Do we want Data localization, including the possibility of incurring greater costs for services, or "Data protectionism" or expensive supply chain security measures applied across many industries?

Do we want to be governed by fear? Do we want national internets, mutual suspicion toward all, indeed a Hobbesian war of all against all? If we agree that we do not, the question becomes: what does the other path, the good path, look like? It is difficult, but we can imagine certain components:

For one, investing in technologies that support data integrity, an issue far more critical than the current fears of privacy. For I can perhaps live with someone knowing my blood type but I cannot possibly live with the fear that it has been changed.

We need genuinely credible legal frameworks, national as well as international and treaty-based, to prevent certain excesses both in terms of backdoors and snooping. This, in turn, will require an international effort, first and foremost, among the liberal democracies, a confidence measure, if you will, to borrow from the security policy term from the Cold War.

This boils down to the need to restore and re-establish what has been lost: trust among allies. Not only NATO allies, but among the countries that believe in freedom, in free and open Internet and in liberal democracy.

None of this will be easy, especially as the adversary in cyber is amorphous, difficult to ascertain and identify. We all too often face what in the past I have called a unique Public Private Partnership between authoritarian governments and organized crime, the former using deniability, the latter enjoying government protection and income. We saw it here in 2007. Today we turn the definition around, in the light of Crimea, and call these attackers "the Little Green Men of Cyberspace". And then, of course, there are the Robin Hoods and their Merry Men who act not on secret contracts with despotic regimes but rather on their own, based on a sense of moral superiority that places them higher than others, including democratically elected authorities.

Yet, if we don't agree among ourselves what is acceptable and what is not, we shall go the route I outlined in my dystopian path. It is important to keep this in mind when we begin to ponder our response and counter-measures to the numerous and genuine cyber threats to our societies.

In other words, in short: when we go the route of Active Defense, the theme of this year's conference, we'd better know what we're doing.