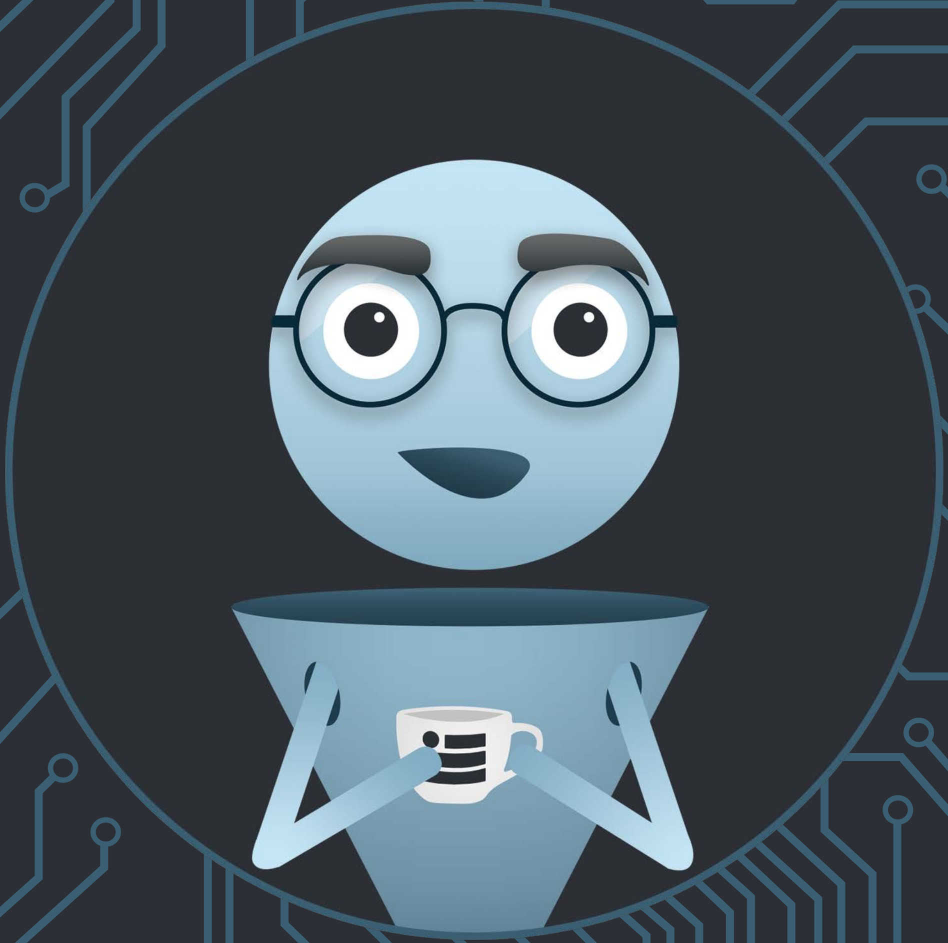
NEW AMERICA

CYBERSECURITY INITIATIVE



DAN WARD & ROBERT MORGUS

Professor Cy Burr’s Graphic Guide to:

INTERNATIONAL CYBER NORMS

NOVEMBER 2016

About the Authors

Dan Ward is the author of two books: *The Simplicity Cycle: A Field Guide To Making Things Better Without Making Them Worse* (Harper Business, 2015) and *F.A.S.T.: How Fast, Inexpensive, Restrained, and Elegant Methods Ignite Innovation* (Harper Business, 2014). He served in the U.S. Air Force for 20 years, holds three engineering degrees, and loves making comics.

Robert Morgus is a policy analyst with New America's Cybersecurity Initiative, where he researches and writes at the intersection of cybersecurity and international affairs. His current work focuses on incident response and crisis management, international norms development, and cyber risk and insurance.

About the Artist

Breck Wills was a graphic design intern at New America. She is a student at Boston College studying Economics, Studio Art, and Computer Science.

Acknowledgements

The authors would like to thank Joanne Zalatoris for bearing with us throughout the process of building this guide. In addition, we'd like to thank Duncan Hollis, Elaine Korzak, Martha Finnemore, and Jim Lewis for their constructive feedback.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies, and for individuals.

Find out more at **newamerica.org/cybersecurity-initiative**.

Let's talk about

Cybersecurity Norms.

Specifically, what they are, how they form, and— most importantly— why they matter?

Let's start with the basics. We all want a nice, safe, stable world...

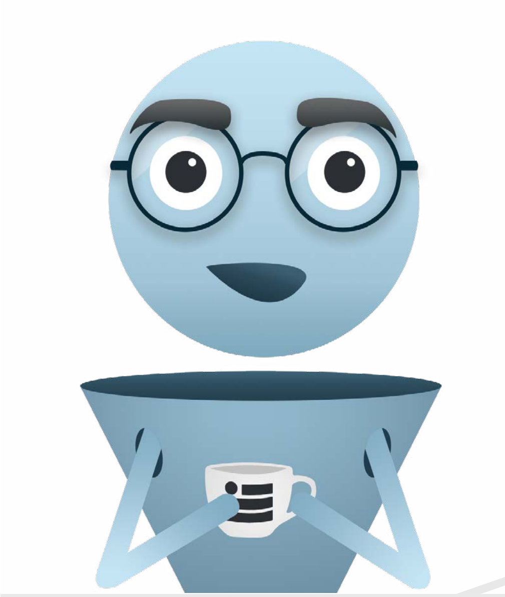
...where bad guys don't do bad things, right?

Norms can help us move in that direction.

Internationally, norms are one of three **tools** available to limit destructive behavior by bad actors.

The other two are **coercion** and **treaties** or laws, and these haven't quite had the desired effect in cyberspace.

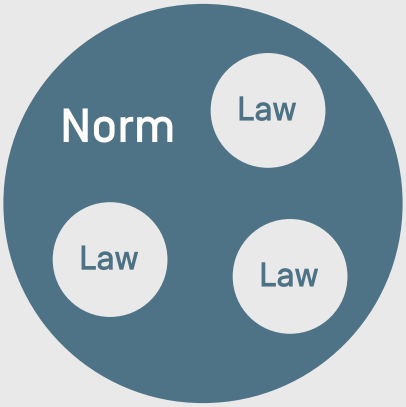
NORMS
COERCION
TREATIES



Though it's worth noting that these categorizations aren't mutually exclusive.

In fact, they often overlap or work in tandem with one another.

For example, an international law probably won't work unless it resembles part or all of an existing norm.



As we'll see, norms help establish and maintain a stable ecosystem.

This is particularly important for an emerging domain like cyberspace, where we are still figuring out how to get along and what the rules should be.

“We’re in the relative infancy of thinking about this issue.“

That’s Chris Painter, and he should know. Mr. Painter leads much of the U.S.’s work on cyber norms.

Norms exist in a variety of domains, and accomplish several important functions

- Deter bad actors
- Define acceptable and unacceptable behaviors
- Help people co-exist productively
- Create new actors or communities around a common identity

But what is a norm, exactly?

In the 1980s Norm was a character on the popular sitcom Cheers.

Everybody knew his name.

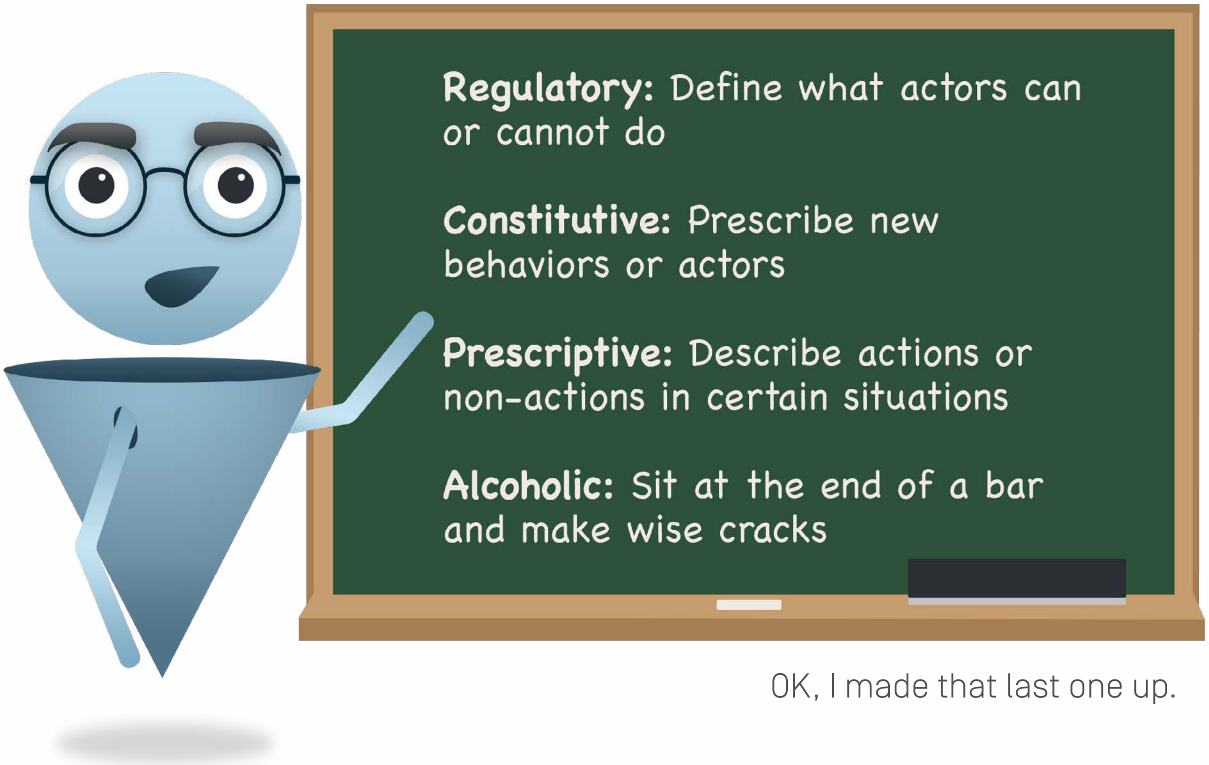
We might even say Norm was...a norm.

Norm is short for normative behavior.

For our purposes, the formal definition of a norm is “collective expectations for proper behavior of actors with a given identity.”

On Cheers, the norm was for actual actors to say “Norm” when the actor playing Norm walked through the door.

In the real world, norms are usually voluntary, non-binding guidelines, and they come in several flavors.



Regulatory: Define what actors can or cannot do

Constitutive: Prescribe new behaviors or actors

Prescriptive: Describe actions or non-actions in certain situations

Alcoholic: Sit at the end of a bar and make wise cracks

OK, I made that last one up.

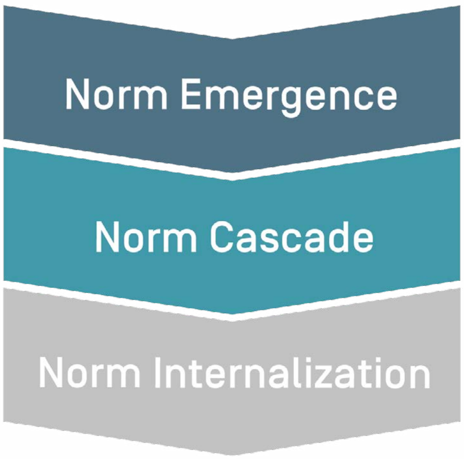
In any domain, as norms develop and spread, they move through a standard lifecycle.

When a norm is first defined and adopted, we say it is in the **Norm Emergence Phase**.

As it is adopted more widely, it moves into the **Norm Cascade Phase**.

Some argue that this cascade is more of a cycle since new norms often grow out of problems with, and disputes about, existing norms.

The point is, as a new norm emerges, it has to spread or it may fizzle and die.



Norm Emergence

Norm Cascade

Norm Internalization

In the final phase of the lifecycle, a lucky norm becomes so widespread and natural that we hardly even notice it, the Norm Internalization Phase.

Not to be confused with the part of the show where Norm internalizes a beer.

Enter Bar
Say "Hi All"
Everyone Says Norm!
Get Beer
Internalize Beer

Several factors can impact the development and spread of a norm.

Some states adopt a norm to convey **legitimacy** and signal a commitment to global citizenship or leadership.

For example, concerned about their record as an aggressor state after WWII, the Japanese adopted a norm of pacifism and demilitarization.

Norms held by powerful entities like the United States are more likely to be widely adopted, so **prominence** is a big factor as well.

I want you to comply with my norm.

Sometimes a norm's **intrinsic qualities** just feel right or moral.

Princess Diana's International Campaign to Ban Landmines appealed to the intrinsic qualities of a norm that limits bodily harm to innocent bystanders in a warzone.

Shouldn't we all comply with this norm?

Often new norms spread out of existing ones. This **adjacency** can help it spread more quickly.

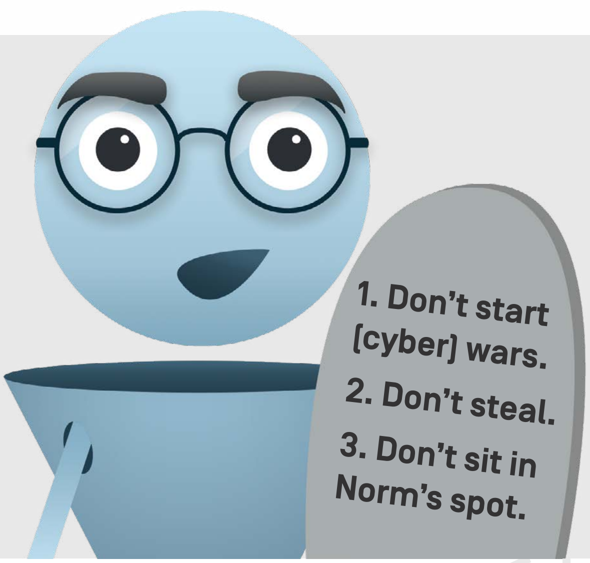
In other words, we already comply with a norm against the use of chemical weapons, so let's comply with a norm against the use of biological weapons too.

Finally, what is going on in the world can drive adoption.

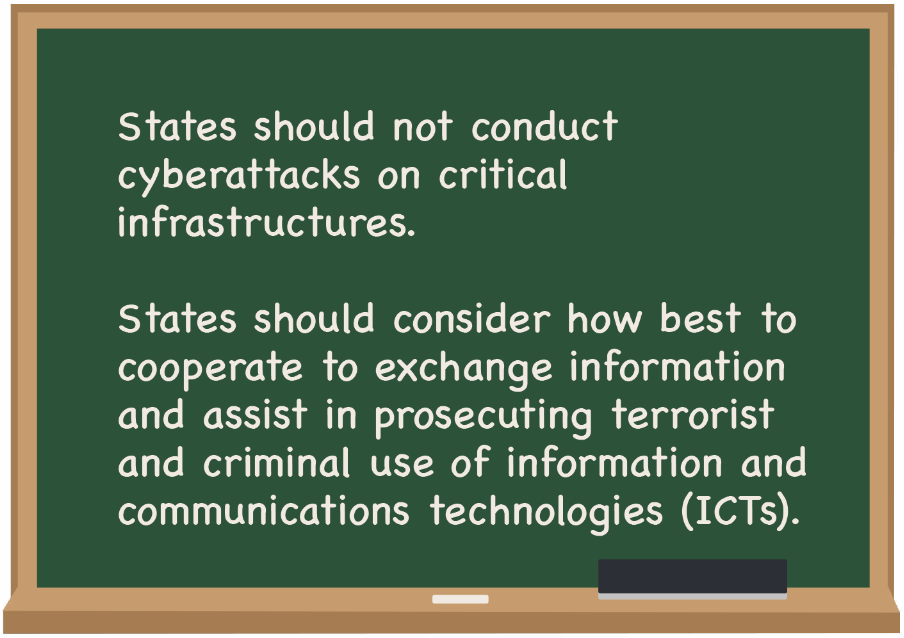
The advancement of ICTs, which enable a more rapid flow of information, has shrunk the time it takes for norms to cascade once they emerge. For example, **a norm against the use of chemical weapons rose to prominence in the aftermath of WWI**, which saw the first widespread use of chemical weapons in warfare.

OK, what does this have to do with cybersecurity?

Well, some norms apply pretty much anywhere, including in cyber.



There are new, cyber-specific norms as well.



States should not conduct cyberattacks on critical infrastructures.

States should consider how best to cooperate to exchange information and assist in prosecuting terrorist and criminal use of information and communications technologies (ICTs).

One question to consider is whether we can just use existing norms...

Or whether we need to establish entirely new ones. Most recently, these discussions have centered around managing conflict.

Western governments generally hold that existing laws and norms are relevant and applicable.

Meanwhile, Russia, China, and other Shanghai Cooperation Organization (SCO) members have pushed for the creation of an entirely new body of law for cyberspace.

Both sides have a point. The truth is, we can use existing norms **and** we need to make some new ones.

In 2010, the United Nations organized a Group of Governmental Experts (GGE) to weigh in on this question.

In 2013, they reached a general conclusion: existing norms and laws apply in cyberspace.

However, recently the Chinese have backtracked a bit.

For those who think that existing norms and laws are the ones that should apply, the questions remains about how that looks in practice.

Enter the Tallinn Manual.

In 2013, a panel of international law experts at NATO's CCDCOE issued the Tallinn Manual, an academic, non-binding study on how international law applies to cyber conflict.

It aimed to help translate and apply international norms to the virtual battlefield.

These processes have left some holes, which a handful of groups are working to address.

Its worth noting that, as we've discussed previously, norm creation is quite different from lawmaking. Nonetheless...

Russia and China, along with a number of smaller states, have suggested developing an entirely new body of international law for cyberspace, with the UN playing a central role.

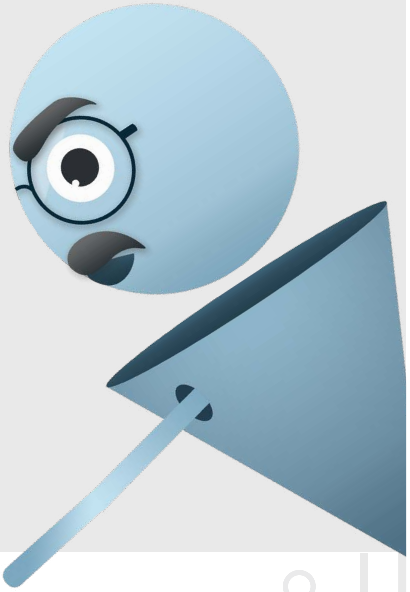
Some feel that the issue is so large that we need to tackle it in bite-sized chunks...

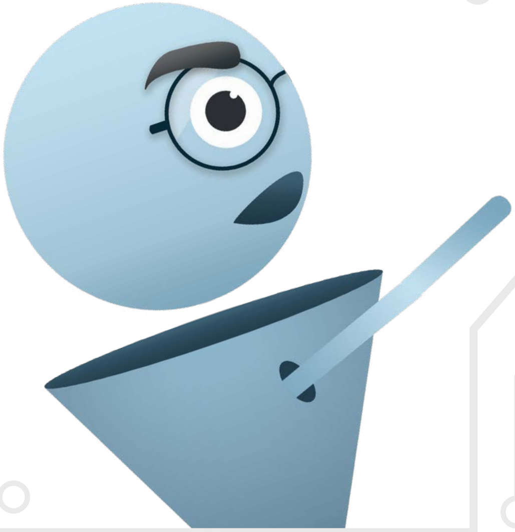
For example, some argue we should focus on discrete issues.

The Council of Europe’s 2001 Convention on Cybercrime aimed to provide some rules of the road specifically for cyber crime.

The Budapest Convention, as it has come to be known, has 50 signatories and seeks to set up a fast and effective regime for international cooperation on cybercrime.

Advocates of this approach attest that we should focus on building confidence around mutually agreeable norms before moving more highly contested issues.





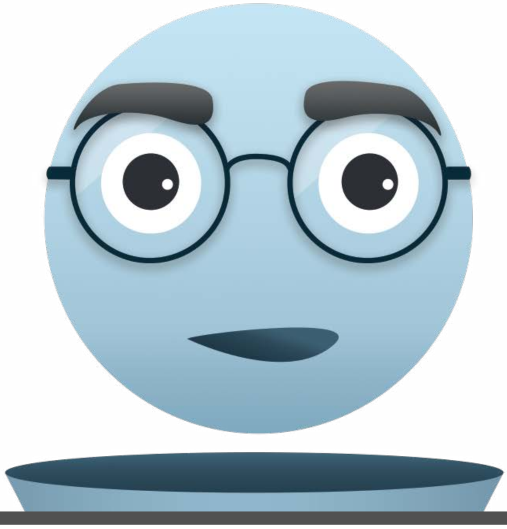
Others would like to tackle the issues on a regional level.

For example, the ASEAN Regional Forum (ARF) is being used as a platform to discuss the SCO’s code of conduct with a wider set of stakeholders and as a platform for bilateral dialogues, in addition to working on regional-specific confidence building measures (CBMs) of their own.

And then there’s the challenge of actually getting actors to abide by the norms.

We can’t just hand them a script and expect everyone to comply

The challenge of implementing norms involves figuring out how to take political, non-binding statements and operationalize them.



Remember, norms are voluntary, non-binding guidelines.

States and other actors have to **want** or be coerced to adopt them.

To see what the future holds for cyber norms, let’s look at some current efforts.

There are **multilateral**, **bilateral**, **unilateral,** and **non-governmental** activities going on.

The **multilateral** front includes work in a number of international forums and organizations, including the UN, SCO, Organization for Security and Co-operation in Europe (OSCE), and others, much of which we’ve already touched on.

The UN's GGE is also making plans to continue studying existing and potential threats...

Along with proposing cooperative measures to address those threats.

Building broad consensus is tough, and the range of possible compromise achievable within the GGE framework may have been exhausted already. At least, that's the opinion of Russia's lead negotiator.

SCO members continue to update the Code of Conduct and propose it to the UN GA as a credible alternative to more occidental normative proposals.

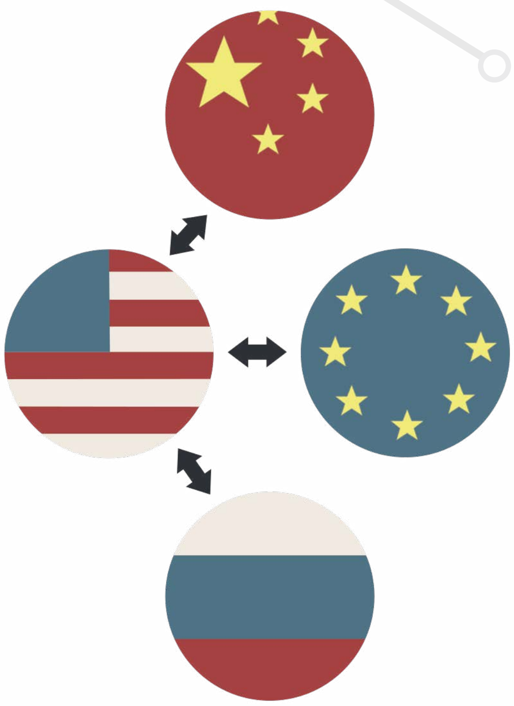
Such as the ARF in Singapore, which is working to operationalize cyber confidence-building measures in Asia.

The OSCE is doing the same in Europe.

Global and regional powers are championing various norms, via the UN, EU, OSCE, and ARF.

There are some regional efforts to implement cyber norms.

The OSCE has published two rounds of CBMs, one in May 2013 and the other in March 2016. The CBMs include things like voluntary information sharing, agreeing on common definitions, establishing and maintaining a national point of contact for incident response, and others.



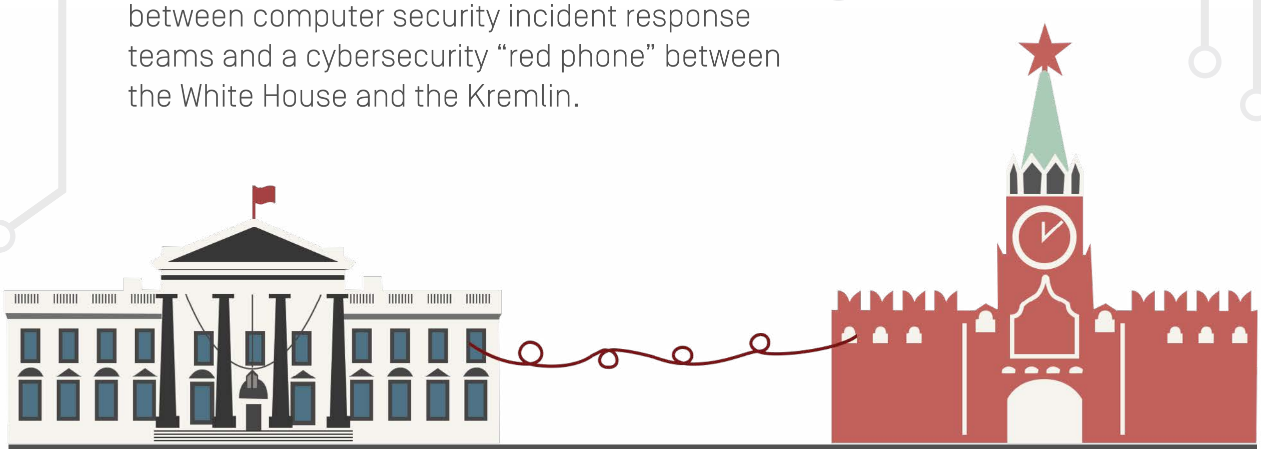
And bilateral discussions continue between the U.S. and China, the U.S. and the EU, the U.S. and Russia, and many others.

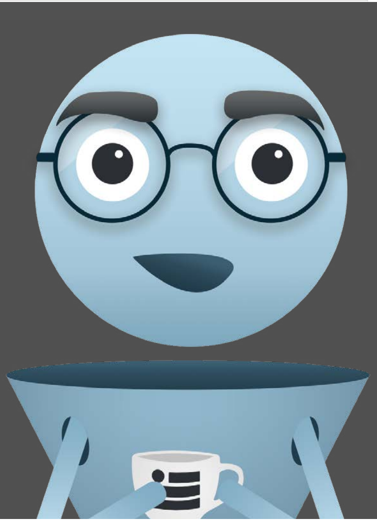
The so-called Obama-Xi pact aims to eliminate the longstanding issue of industrial espionage between the US and China.

Prior to reaching this agreement, China had not accepted industrial espionage as off limits. However, the pact, along with some minor public shaming, G8 recognition of the problem, domestic factors, and indictments of individuals carrying out the acts made it next to impossible for China to not comply.

And in 2013, the U.S. and Russia agreed to a series of bilateral CBMs.

These include items like creating formal links between computer security incident response teams and a cybersecurity “red phone” between the White House and the Kremlin.





Sometimes, **not** doing something can inadvertently create an undesirable norm.

That can create pressure for states to act **unilaterally.**

One example of this happened in May 2014, when the US filed criminal charges against military hackers from China.

This unilateral legal action is the first time known state actors were charged with a cybercrime. These indictments signaled that the U.S. would no longer “do nothing” and allow a norm letting states conduct industrial espionage form.

Gradually, the Chinese military scaled back their hacking activities.

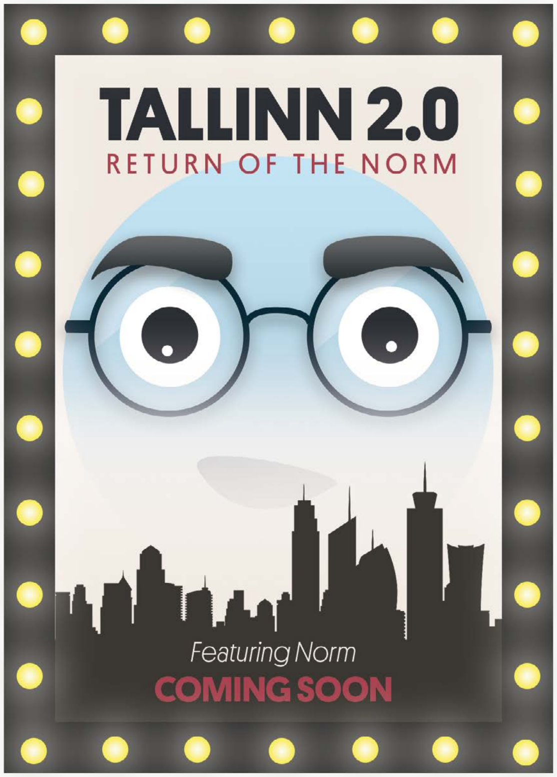
See, it worked!

Not so fast. The indictments weren’t the only factor here.

There was also the aforementioned Obama-Xi pact, multilateral dialogues in the G7 and elsewhere, and a growing sense the US was nearing its breaking point.

Is this an emerging norm or two or seven? Hard to tell, but one thing is clear:

Norms don’t develop in a vacuum.



Some non-governmental efforts are also ongoing. For example, they are making a sequel to the Tallinn report.

Tallinn 2.0 [*Return of the Norm*] is due to be completed in late 2016.

How will the sequel differ? Well, Tallinn 1.0 focused on translating **laws of war** to cyberspace.

Tallinn 2.0 aims to interpret international law **outside of armed conflict** for application to cyberspace.

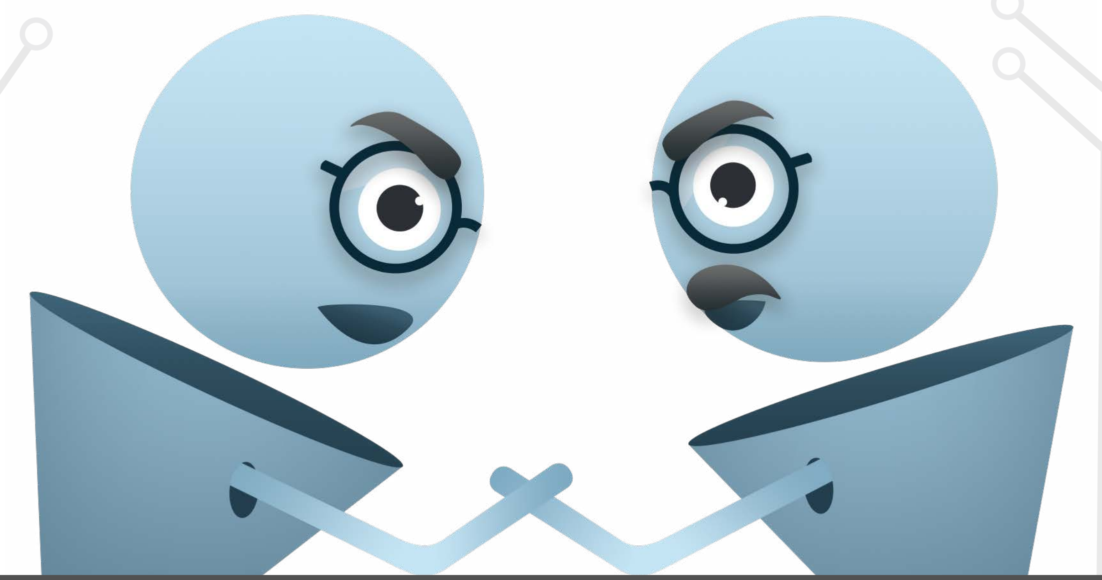
However, it remains to be seen whether Tallinn 2.0 will have an impact like the original Tallinn Manual. Currently, it lacks the same level of international support.

All together, these efforts create opportunities for new norms to develop.

We can't exactly predict or control how that development progresses. There are just too many factors to consider.

Having said that, norms development is a dynamic, ongoing process and we know some efforts will carry norms into the future.

Which norms will prevail? Hard to say.



But as we've already noted, some factors increase a norm's chances of success.

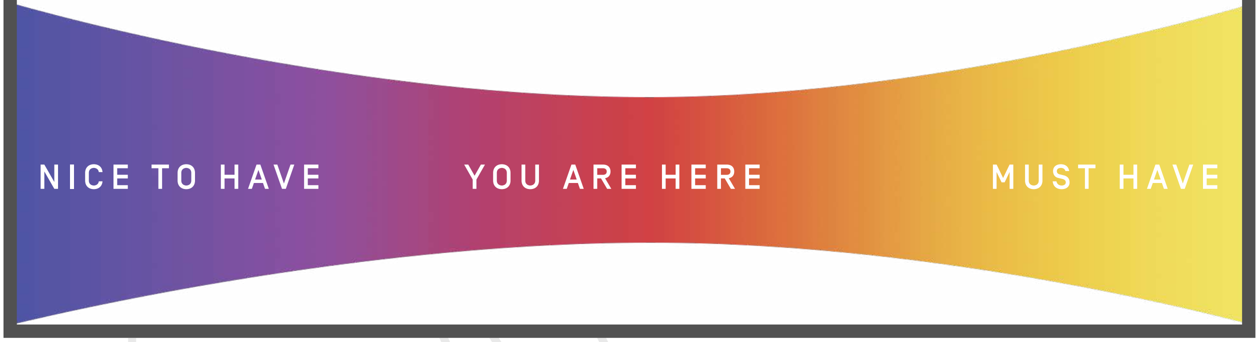
These factors include the **legitimacy** and **prominence** of norm advocates.

The **intrinsic qualities** of the norm, or its **adjacency** to an existing norm also play a role.

And **world events** can make a norm more or less appealing.

How much does this matter? Are norms essential, or just nice to have?

The answer is somewhere in the middle.



Norms can be a helpful first step towards more formal agreements and treaties, as was the case with landmines, though they don't always have to become more formalized to be effective.

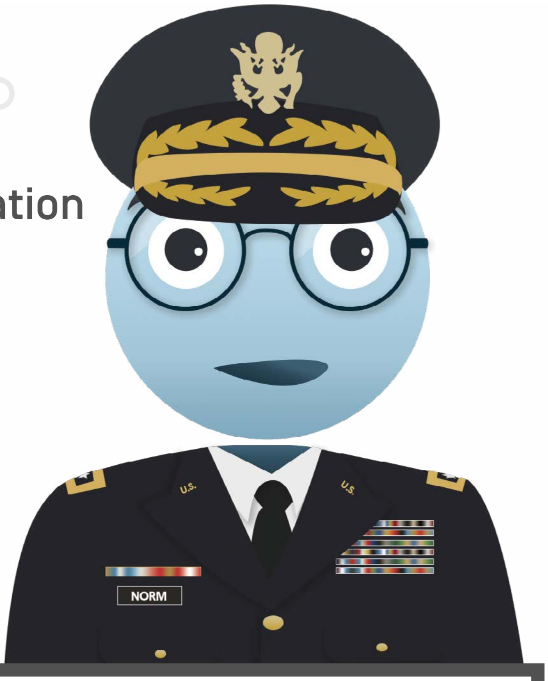
They can foster critical thinking and stability.

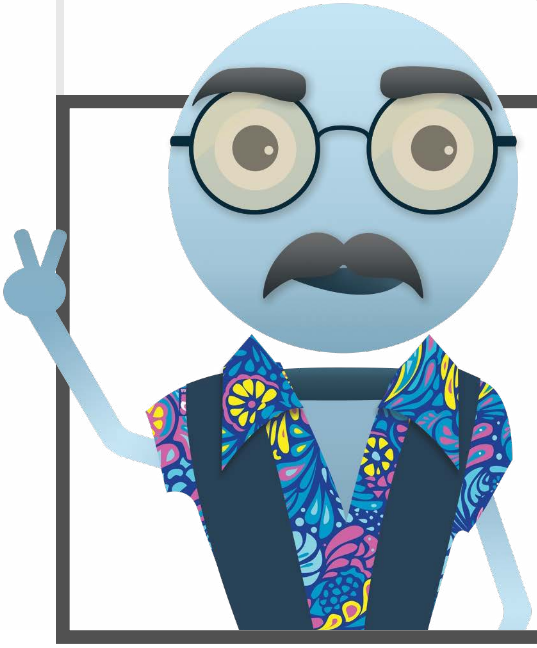
But as we've noted, they are usually voluntary.

Norms **influence** behavior rather than demand or enforce specific actions.

And so far, most of the conversation about cyber norms has revolved around state-on-state conflict.

However, cyber norms are beginning to emerge in other forums...





Norms for how we govern the internet were proposed at NetMundial in 2014 in Brazil.

The multistakeholder participatory model used at Net Mundial was designed, in part, to **demilitarize discussions** around the formation of global cyber norms by engaging participants from industry, academia, and civil society, in addition to traditional state bodies.

Increasingly, non-state actors can impact the norms process. Private companies, like Microsoft, have begun to take a leading role in crafting and proposing new norms.

States aren't the only ones who can be norm entrepreneurs, especially in cyber, where the norms affect state and non-state actors alike!

Yup, there is a lot of work still to be done...

In conclusion, norms are important and useful. They help define expectations for proper behavior.

By providing guidelines, they can discourage bad actors from acting badly...

And can even serve as a foundation for more formal treaties and agreements.

A well established collection of norms gets everyone on the same script. We might even say they... set the bar.

And norms make sure we all know what to do when that guy walks into that bar. You know his name, right?