Steve Cooper

Handout #7
July 7, 2016

Cybersecurity Policy

Dates:

Rough draft of policy paper due Wednesday, July 13
Policy paper returned by Thursday/Friday, July 14/15
Policy paper rewrites due Monday, July 25

Supposed you are called to serve on an expert panel convened by the Standing Committee of the National People's Congress (NPC). You are being asked to present a single, coherent policy the task force can discuss, and forward to Chinese Communist Party (CCP) for adoption. Your policy recommendation must focus on China, or Chinese relations with other countries, but other than that, can recommend almost anything relating to cybersecurity policy. The United States government has created many documents detailing high-level policy recommendations. (The Chinese government may also have similar documents, but I am unable to read Chinese). My hope is that some of these documents may give you a high-level idea about a policy you could develop. You may wish to take a look at some of the following:

60 Day Cyberspace Policy Review (Hathaway, 2009)
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The Comprehensive National Cybersecurity Initiative (CNCI)
http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

National Initiative for Cybersecurity Education (NICE) 2010
http://www.whitehouse.gov/sites/default/files/rss_viewer/cybersecurity_niceeducation.pdf

Cybersecurity, Innovation and the Internet Economy (Department of Commerce, 2011)
http://www.commerce.gov/sites/default/files/documents/2011/june/cybersecurity_green_paper_finalversion_0.pdf

Cybersecurity - Continued Attention Needed to Protect Our Nation's Critical Infrastructure (GAO recommendations, 2011)
http://www.gao.gov/assets/130/126702.pdf

Other possibly useful government links:
Council on Foreign Relations Cybersecurity policy page:
http://www.cfr.org/cybersecurity/cybersecurity-policy/p27480

White House page on cybersecurity
http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

The problem with these documents is that while they provide many good ideas (it is likely that the policy you'll be recommending will be mentioned at some level in one or more of these documents), the ideas are almost always too vague so as to be able to recommend a policy that could actually be implemented.

When faced with reports of this sort, governmental committees and government agencies often try to develop more specific (and implementable) policy by convening expert panels to discuss the question in detail. Typically, the expert panel meets initially in a face-to-face session to frame the issues, but then conducts most of its actual work through electronic mail before meeting for a final time to discuss recommendations.

Imagine that you have just been appointed as a member of such an expert panel. Your job is to ***make a single detailed policy recommendation***. The intent is that your recommendation is sufficiently detailed that it could actually be implemented. You will write a 5 page briefing report (plus a one-page executive summary) outlining your findings.

When a policy panel first seeks to confront an issue, the best thing to do is to begin in an information-gathering mode. There is a great deal of background material on this subject. Hathaway's report, in particular, identifies many of the sources her experts used in preparing the report. This could provide a good starting point for you.

Requirements for the paper

Your paper should present a particular policy position and your own defense of it. An important part of the policy position is that you need to both defend your particular position as well as justify why it is the "right" position to take. Often this can be accomplished by considering reasonable alternatives to your position, and then arguing (writing about) the deficiencies in those alternate positions.

As always, you need to keep your audience in mind. Remember that the scenario here is that your panel is preparing briefing papers for policymakers who do not understand computing technology well but are aware that the level of fear/concern among particular interest groups is high. Moreover, given that your audience is a group of busy people who may not have a chance to read your report in full, it is strategically important to make sure that your main ideas are easy to find. Starting off with a concise executive summary is essential, but section headings and bullet points can also be useful in this regard.

Your paper must include the following:

- An executive summary that outlines the central elements of your proposal. This summary must fit on a single page of the report.
- Immediately following your executive summary is the five page paper. Note that your paper should not exceed five pages (excluding the executive summary and references).
- A list of additional references that you have used to develop your position. You should use at least three sources, not including the reports listed above.

- Please make sure you provide inline citations.

A note of warning: In order for your policy recommendation to be implementable, it must be reasonable.

You should format your paper using double-spaced text set in Times New Roman 12 with the default margins in Microsoft Word® (1.25" on the sides, 1" at the top and bottom).

Submission

You should e-mail me your paper. I would also like you to provide me with a hardcopy of your paper.

Some thoughts about writing a strong policy paper: Well written policy papers often look the same structurally. This makes them easy to read, and it also is a feature of them needing to make a persuasive argument in a short amount of space. You are not required to follow this outline, but it might help you avoid making big mistakes.

Background Information (0.5 pages to 1 page)

Your reader is a policymaker. They know little about computers. You don't need to explain basic stuff, but you do need to explain why they should care about your specific subset of cybersecurity given that their constituents are asking for more money on things like education and roads and they aren't asking for cybersecurity.

This should be specific to your proposal, not generic. If you are writing about people stealing passport data via RFID, for instance, you could spend one sentence describing the technology, one sentence describing the attack, and two sentences describing the impact (economic losses, security vulnerabilities).

The bottom line: a policymaker without much prior knowledge should understand why the problem you're fixing is a problem that needs to be fixed.

Proposal (0.5 pages to 1 page)

You aren't writing the actual law that would go to the CCP. Since this paper is so short, neither are you writing the full justification for such a law. Rather, you are writing a proposal that will prove to a policymaker that doing a full analysis and writing a law are both good ideas. To be clear, however, this doesn't mean that you can push away all detail with the idea that it would be in a further analysis. The distinction is that with this paper, you are convincing a policymaker who trusts you; the later analysis would be for that policymaker to convince people who might not them.

You don't need to spell out every bit of minutia ("and applicants will need to fill out a form 990B in order to establish eligibility for..." is going too far). You do need to be very close to implementable, though. For instance, if you are allocating funds, you might not need to get the exact number, but you should get within a reasonable range. A $5-10 million proposal is very different from a $50-100 million proposal, but a $6 million proposal is probably not too different from a $9 million proposal.

The bottom line: it must be detailed enough that a policymaker would know how to implement it without too much extra research.

Justifications for your Proposal (2.5-3.5 pages)
Why is your proposal good? How many lives would it save? How much money? Would it improve our economic competitiveness for years? There are plenty of ways to measure impact. Make sure that you have at least one compelling measure of impact that you defend well and with lots of data and evidence.

Specificity counts! You are a research aide, not an expert. That means that if you're doing a lot of your own analysis to connect the dots, we won't be as likely to believe you as if you found an expert at a think tank who defends your specific policy.

The bottom line: convince us that your policy is good.

Alternatives (0.5-1.5 pages)
You identified a problem and you presented a solution to it. It probably isn't the only solution. Different authors present different solutions since these are very complicated problems.

If your solution is the only solution, there will still be different ways to go about it. There might be different technical proposals; there might be different agencies that could do it; there might be different timeframes. There isn't one specific thing that you should focus on. Rather, you should consider the most relevant comparison for your specific focus area.

The bottom line: don't just convince us that your policy is good; convince us that it's the best.

One of my former Stanford TAs wrote a response to some students who were asking about the policy paper in a previous quarter. (The Stanford students were asked to make a proposal for the US Congress.) I quote his response nearly verbatim below.

Many students have asked questions about the policy paper. The most common question is similar to the following:

> I want to write about cybersecurity education. However, I looked online and found that the government is already doing that with their Stop Think Connect program! Can I pretend that my paper was being written in 2009? What should I do?

I am Senator Smith (D-OR). You are one of my research aides. I have to go to the media on October 28, 2013 at 5pm with my cybersecurity proposal. I have tasked you with writing that proposal. If your proposal tells me to establish a program that already exists, it's going to make me look bad, so don't do it.

However, don't let that constrain you! The Hathaway paper, for example, has 70 pages of unsolved problems. Just because the government has started to implement potential solutions to ten of those problems doesn't mean that all 70 pages of problems

are solved. In fact, it probably doesn't mean that those 10 candidate proposals are solved. Cybersecurity is an unsolved problem. If Stop Think Connect had solved cybersecurity education, we would live in a very different world than we do today.

One thing you could do is take an existing program and describe how to improve it. Then, I will look at your research and the costs and the benefits and choose whether or not to propose those specific changes to that specific program. Or, you could talk about a program that doesn't exist at all.

Keep in mind that the above mentioned government documents, though long, are also extremely vague. Cybersecurity could mean a hundred different things in a hundred different papers. If, in your paper, you treat cybersecurity as one thing, you probably aren't being specific enough to make a well defended policy proposal. For instance, are you educating me about phishing? About HTTPS? About DNS MITM attacks? Or, if you're proposing making the internet more secure, are you doing that with IPSEC, with DNSSEC, with a Web of Trust, with fewer CAs, with a provably exponential time encryption algorithm, or with something else? Or, are you talking about a completely different domain such as cybersecurity for satellites, pentagon computers, the DMV, or the RFID chips in everyone's passports?

And all of that is just talking about the problems! There are also tons and tons of ways to implement a solution for every single one of those problems. With the issue of RFIDs in passports, for instance, should I change RFID to NFC and use encryption? Should I remove RFID chips entirely? Should I require two factor authentication? Should I add biometrics? Should I encourage everyone to get containers for their passports that act as faraday cages so that the RFIDs can't easily be snooped?

Right now, we're pretty much in the wild west of cybersecurity. You can't throw a rock without hitting an unsolved problem, either technical or policy. This is an exciting time to be alive and an exciting thing to write a paper about (which you could actually get published and which could actually affect policy!). Make us proud.