INFORMATION WARFARE THREAT DEMANDS MORE ATTENTION ON ALL SIDES

An interview with Senator Jon Kyl

Neither the administration, nor the Congress, nor the public at large is devoting enough serious attention to the growing threat of information warfare, says Senator Jon Kyl. Potential adversaries are honing their ability to attack the critical infrastructure that increasingly runs the nation's communications, transportation, and financial systems — and its vital defense establishment as well, he warns. Kyl, an Arizona Republican, serves as chairman of the Subcommittee on Technology, Terrorism, and Government Information of the Senate Judiciary Committee. He also is a member of the Senate Select Committee on Intelligence. Kyl was interviewed by Contributing Editor Ralph Dannheisser.

Question: At a committee hearing in June, you said that the United States' "soft, digital underbelly" is more readily vulnerable to attack than the nation's military. Could you elaborate on that a bit?

Kyl: I think that's generally recognized as true. We've got the strongest military in the world, and there's nobody that's really capable of taking us on. So the question is: Would a potential adversary seek the more vulnerable spots to attack the United States if they wanted to do so? The same thing for terrorists. And the answer is that among the vulnerabilities that we have is our information infrastructure, because we are reliant more than any other nation on high technology for our communications, our transportation, our financial dealings — including, of course, our defense establishment. And as a result, the vulnerability that our information infrastructure has is probably one of those key target points for either an aggressor state or a terrorist organization.

Q: Along the same lines, you have said that this is the most difficult and important national security and public safety concern that our country's leadership will face in the years ahead. What are some of your worst-case fears if the issue is not properly addressed?

Kyl: Let's start with the transition to the new millennium. The Y2K (year 2000 computer) problem, which has been rightly identified as a serious potential problem for the country, is exacerbated by the fact that it will present terrorists or other groups of people or individuals who mean us harm a golden opportunity to attack at the time of maximum confusion. We will not know why the many things that are going wrong at midnight, December 31, 1999, are going wrong. We will presumably attribute most of the problems to Y2K computer glitches, but obviously it represents a great opportunity for sabotage or other attack on our infrastructure by those who mean us harm — both because their activities are covered by the event and also because of the vulnerability that the event itself presents.

So there's the first great opportunity. But apart from just that moment in time — because, as I said, of the vulnerability of the different aspects of our civil society as well as certain defense components — attacking our infrastructure represents one of the best ways of doing us harm in the abstract and, in a situation where there is an ongoing conflict, represents a great opportunity to disrupt our ability to meet the threats involved in that contingency.

Q: Overall, how easy is it to break into the information grid at some point, and what sort of damage could someone who succeeds in that effort do?

Kyl: Well, it's surprisingly easy. It's hard to quantify that in words, but there have been some exercises run recently. One that's been in the media, called "Eligible Receiver," demonstrated in real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by, literally, hackers — people using conventional equipment, no "spook" stuff in other words. Just that which is available can disrupt key aspects of

our information infrastructure. Now, in this case, they disrupted parts of the electric grid, the transportation system, the financial system. Others that are vulnerable include things like water systems, all forms of telecommunications, of course, and the emergency response people, but perhaps from the defense point of view nothing is more serious than the labs of the defense establishment itself as well as weapons systems.

So, there is a high degree of vulnerability, and each time some youthful hacker from another country breaks into the Pentagon computer system, people scratch their heads and wonder how it can happen and they learn from the exercise. But it seems that it's a constant learning process. Another illustration: just before the dust-up last February in Iraq, where we were about to go in and do something to Saddam Hussein, the hacking into the Pentagon computers was so significant that the president was actually advised that the activity could be the result of an intentional action by the Iraqi government. For a while we did not know whether that was the cause of this or not. It turned out to be three young men in three different countries. So to respond to the question — "How vulnerable are we?" — I think that helps to illustrate the point.

Q: Certainly the fact that these young guys with no sinister motives can get in that easily would suggest that our adversaries could do it as easily with significantly more prospect of damage.

Kyl: That's exactly the concern.

Q: From your own perspective with the committee and having a keen interest in the topic, how do you see the Congress' role in protecting against this sort of information warfare or cyberterrorism?

Kyl: Well, the obvious — we have to give the national security agencies, the defense establishment, enough money to deal with the problem and the authority to deal with it.

There are some real issues involved, but I think that from a public policy standpoint, it's primarily to establish the policy for the government, to take it seriously, and to provide the means of doing so.

Now, we have been prodding the (Clinton) administration for four years, and it's still behind the curve. It was supposed to present a plan, and that hasn't been accomplished yet. What the president did, in an executive order, was to order in 180 days a plan to be prepared. So we're awaiting that. November 22 would be the due date. So presumably that's the agencies' plan for dealing with this among themselves.

Q: That was at the instigation of the Congress?

Kyl: The Congress got the ball rolling, by twice requesting, or requiring, the president to submit a plan or a report. He didn't do that. Instead he appointed a commission, first of all, and as part of that he also appointed a task force within the government. Among the recommendations that they made was to prepare this plan. And so they've been planning to begin to commence to start to report here for a long time, and we're about to the end of that 180-day process now. I'm hopeful that that plan will at least provide the direction for each key government agency, in dealing with the private sector that it has relationships with, to provide the guidance for at least the first phase of activity. But missing from that is still a significant part of the defense component, which I think the administration is going to have to focus on next. So our role, I think, is to continue to prod and provide whatever resources are necessary.

Q: Do you feel the issue is getting the legislative attention that is required for that purpose?

Kyl: No. But there hasn't been disagreement in the legislative branch. It's been a bipartisan, bicameral effort. So there's not a problem there. But if you ask — "Is there enough understanding of the issue, either in Congress or in the public generally?" — the answer is "No." And there's not enough understanding or commitment from the administration either.

Q: You alluded to this peripherally, but given the interconnectedness of the information infrastructure, is there a need for the public and private sectors to somehow coordinate their activities on this and work together?

Kyl: Yes, there is. And part of the plan that we anticipate the administration will be developing is to deal with that element of coordination. For example, the Department of Transportation presumably will have a plan that integrates the private sector components of

the transportation industry with the Department of Transportation for joint response — indications and warning and response — and so on. There is also an industry group that's dealt primarily in the telecommunications area that's had a long-term liaison with the president. They continue to give a lot of advice about what the private sector needs, and what they can do to deal with this. Because ultimately, it's the equipment, the technology generated by the private sector that ends up being used by both the private and the government sectors, and they can be pretty innovative about what they build into their systems and how they offer solutions to the government. They've been doing that.

Q: You mentioned earlier a suspicion at one point, which proved to be unfounded, that Iraq was undertaking some activity in the information warfare area. Do you know of any U.S. adversaries that are actively getting into this sort of preparation, and what would be the nature of that?

KYL: According to our intelligence agencies, there are a large number of countries that are working on information warfare techniques, and a smaller number of countries that have specifically targeted the United States in their planning efforts. I cannot say whether there has ever been an attempt by another country to attack our information infrastructure.

Q: I guess the attacks would occur in either of two ways: Actually knocking out certain areas of activity that are controlled by the information system, or by feeding false information into the systems.

KYL: You could go in and acquire information, you could plant various kinds of bugs that would either disrupt or stop operations, or put in false information. So you could really do all three of those things.

Q: And, presumably, somebody somewhere must at least be looking into that sort of effort.

KYL: As I say, there are a large number of countries that have programs under way, some of which are actually aimed at the United States. Now that's to be distinguished from saying that these countries are attempting to attack the United States today; I'm simply saying that they have developed programs, or are in the process of working on the concept of information warfare against the United States. It would also stand to reason, and this may be your next question, that the United States would be thinking in offensive and defensive terms as well.

Q: Could you expand on that a bit?

KYL: The only thing that I would say further is to remind readers that, of course, with respect to the ability to exercise offensive information warfare, we are by far the most vulnerable country because of the degree of our reliance upon technology, so to us it is really more of a defensive thing than an offensive thing.

Q: But you're suggesting that certainly preparations or investigations are under way here as well.

KYL: Well, remember that there was some information that came out shortly after Desert Storm revealing a degree of U.S. disruption of Iraqi communications and other activities which I guess one can say was maybe the first example of the use of information warfare. It's actually not something new. I mean for years, for decades, we've attempted to disrupt the enemy's communications and break their codes and so on — it's all the same thing. This is just a much more sophisticated version of it.

Q: What are you planning within the subcommittee at this point in terms of further activities?

KYL: The next thing we will do is to review the report that's issued in November in response to the Presidential Decision Directive (PDD) which will give us some indication of where the administration is planning to go, evaluate that, perhaps hold a hearing to learn what they're intending there and perhaps hear from people who might have other views, and I'm not sure, at this time, what we will do after that.

Q: Do you see large added infusions of funding being necessary at some point?

KYL: Relatively small actually, but there are going to be some funding requirements, I would say.