

The Honorable Jane Harman
Testimony before the House Homeland Security Committee
January 15, 2014

I've always said that terrorists won't stop to check our party registration before they blow us up. One of the hallmarks of my relationship with Chairman Michael McCaul was that we worked closely together to solve problems – we didn't let politics get in the way.

I'd like to make three basic points:

1. I watched closely for many years as al Qaeda and associated terror groups changed. While the US government does not do a perfect job explaining the evolution, we are addressing new threats and in my own view making progress. A promising development is the indigenous push-back against the Islamic State of Iraq and Syria – or ISIS – in Syria. This is reminiscent of the Arab Awakening in Anbar, and might unify the Syrian opposition.

The problem with the US narrative is not that we are underplaying the terror threat. We are inadequately explaining our agenda to people in the US – and in the region. If we leave a vacuum, the bad guys fill it with their narrative.

2. Secretary John Kerry's efforts to negotiate peace in the Middle East and a nuclear deal with Iran are heroic and if successful will have a major impact on stability and security in the region. They will also "reset" how the US is viewed.
3. Since 9/11, there have been almost 400 homegrown terrorists indicted on terror-related charges or killed before they could be indicted. The biggest threats to the US homeland are homegrown, lone-wolf terror attacks and cyber-terror attacks.

a. Lone wolves

- Radicalization is an individualized process and the vulnerable come from varied backgrounds. Recent reports that Syrian extremist groups are recruiting for US attacks are extremely concerning. (See my *LA Times* op-ed dated January 6, 2014).
- Reverse recruitment is also happening, like al Shabaab in Minnesota.

b. Cyber terror

- We are way behind the curve in understanding, responding to, adapting to and preventing cyber intrusions – especially in the private sector. We're just starting to protect better our physical computer systems. But we've barely touched security for mobile devices.
- Snowden leaks have compromised a lot of our technical ability. Some, like former Department of Homeland Security Assistant Secretary for Policy Stewart Baker, suggest that there are many countries that may have used the

leaks to bolster their own capabilities. That means we lose the competitive edge.

- Most terror groups or lone-wolves don't have advanced technical capability yet. But they learned quickly how to use the internet to radicalize, recruit and fundraise; why wouldn't they learn how to launch attacks that way?
- It's not hard to buy exploits and find someone with the expertise to deploy them.
- So we have an opportunity now to harden our critical infrastructure. The President's Executive Order is a good start. But legislation is essential to compel industry to share threat data – not personal information about individuals – with the Department of Homeland Security and provide appropriate immunity when it does.
- HR 624, the Cyber Intelligence Sharing and Protection Act, (Rep. Mike Rogers) has passed the House. HR 756, the Cybersecurity Enhancement Act, (Rep. Mike McCaul) has passed the House. The Senate approach is different and progress is urgently needed.
- Spillover from the Snowden leaks has meant that businesses are even more reluctant to cooperate. We need more brain cells on this problem because it is the key to preventing a catastrophic attack.

So, what to do? Just as we've layered security across ports and transportation systems, we need to do the same in the cyber world. The SAFE Ports Act, a product of the House Homeland Security Committee (Lungren/Harman) in 2006, could be a model – leaving the more controversial pieces for stand-alone legislation.

Conclusion

1. Threats today are different and on a smaller scale. Al Qaeda in the Arabian Peninsula describes this shift in its English-language online magazine Inspire as a “strategy of a thousand cuts.” And they aren't expensive: "Operation Hemorrhage" – AQAP's printer-cartridge bombing attempt – cost less than \$5,000.
2. We need a narrative and whole of government approach more than kinetics.
3. But partisanship is a huge obstacle to progress.