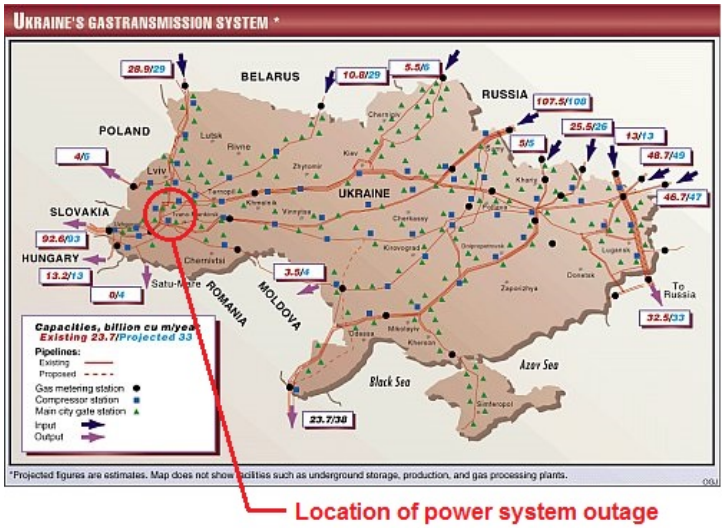
UKRAINE'S POWER SYSTEM HACKING: COORDINATED IN MORE THAN ONE WAY?



[original graphic: outsidethebeltway.com]

Analysis by industrial control team SANS determined hacking of Ukrainian electrical power utilities reported on 23-DEC-2015 was a coordinated attack. It required multiple phases to achieve a sustained loss of electricity to roughly 80,000 customers. SANS reported they "are confident" the following events occurred:

> - *The adversary initiated an intrusion into production SCADA systems*
> - *Infected workstations and servers*
> - *Acted to "blind" the dispatchers*

> - *Acted to damage the SCADA system hosts (servers and workstations)*
> - *Action would have delayed restoration and introduce risk, especially if the SCADA system was essential to coordinate actions*
> - *Action can also make forensics more difficult*
> - *Flooded the call centers to deny customers calling to report power out*

An investigation is still underway, and the following are still subject to confirmation:

> - *The adversaries infected workstations and moved through the environment*
> - *Acted to open breakers and cause the outage (assessed through technical analysis of the Ukrainian SCADA system in comparison to the impact)*
> - *Initiated a possible DDoS on the company websites*

The part that piques my attention is the defeat

of SCADA systems by way of a multiphased attack – not unlike Stuxnet. Hmm…

Another interesting feature of this cyber attack is its location. It's not near sites of militarized hostilities along the border with Russia. where many are of Russian ethnicity, but in the western portion of Ukraine.

More specifically, the affected power company served the Ivano-Frankivsk region, through which a large amount of natural gas is piped toward the EU. Note the map included above, showing the location and direction of pipelines as well as their output volume. Were the pipelines one of the targets of the cyber attack, along with the electricity generation capacity in the region through which the pipes run? Was this hack planned and coordinated not only to take out power and slow response to the outage but to reduce the pipeline output through Ukraine to the EU?