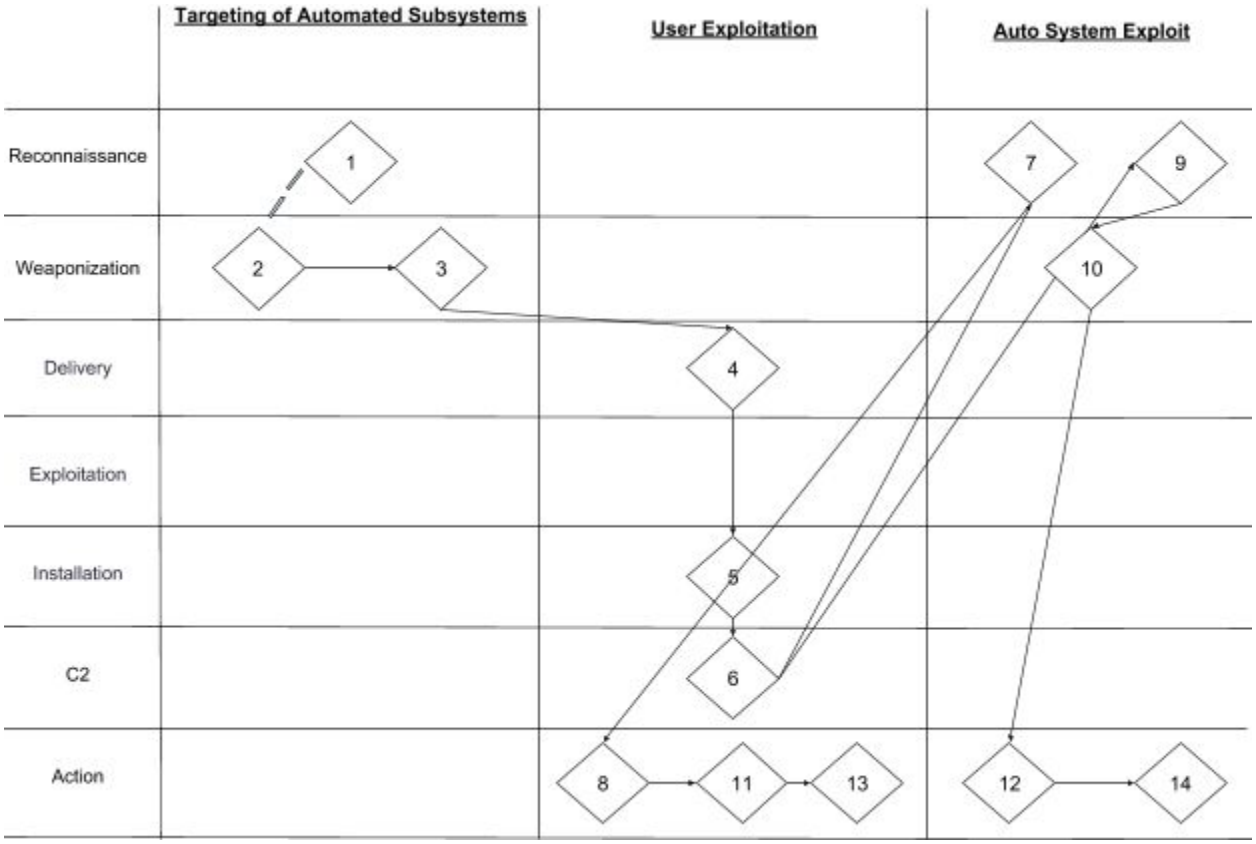
Analysis of the Cyber Attack on the Ukrainian Power Grid:

Alex Miller, Tyler Crosby, and Joshua Bunce



Event	Hypothesis/Actual	Description
1.	**Hypothesis**	Identify highly automated substations.
2.	**Actual**	Altering Microsoft Office documents using BlackEnergy 3 malware.
3.	**Actual**	Crafting phishing emails to look like they are coming from a trusted source to campaign against low-level employees.
4.	**Actual**	End users opening malicious documents.
5.	**Actual**	Vulnerability inside of the Office macro functionality that Allows Black Energy to be installed onto users PC's.

6.	**Actual**	With the use of the Black Energy external IP addresses Are capable of communication into the infected systems. Allowing persistent Command and Control network for Prolonged system enumeration and mapping.
7.	**Hypothesis**	Internal system mapping through established back door to identify exploitation targets and reverse engineer automation controls. Starting to look how to start harvesting credentials, escalating privileges, and moving laterally within the infrastructure.
8.	**Actual**	Leveraged installed persistence to open firewall ports to Allow for RDP connections and remote systems take-over.
9.	**Hypothesis**	Identification and enumeration of serial to ethernet Connectivity and usage.
10.	**Actual**	Using the information gained from the analysis of the field Serial devices to create malware that would control and then Destroy the devices. Testing it on a recreated device In a controlled environment.
11.	**Actual**	Align all controlled devices to execute system command For password change at the same time.
12.	**Actual**	Use HMI's that are inside the SCADA environment the shut off breakers.
13.	**Actual**	Using a modified version of KillDisk to remove the MBR (master boot record). This exploit allowed for the increased Time for recovery and removing evidence.
14.	**Actual**	Overriding of firmware to cause a fatal crash of devices Making them unrecoverable.