Operations Analysis of Cyber Defense Questions Using Data Farming

Dr. Gary Horne
Blue Canopy Group

9th ORA Conference, Presentation Number 7
22 October 2015
Ottobrunn, Germany

Some Recent Background

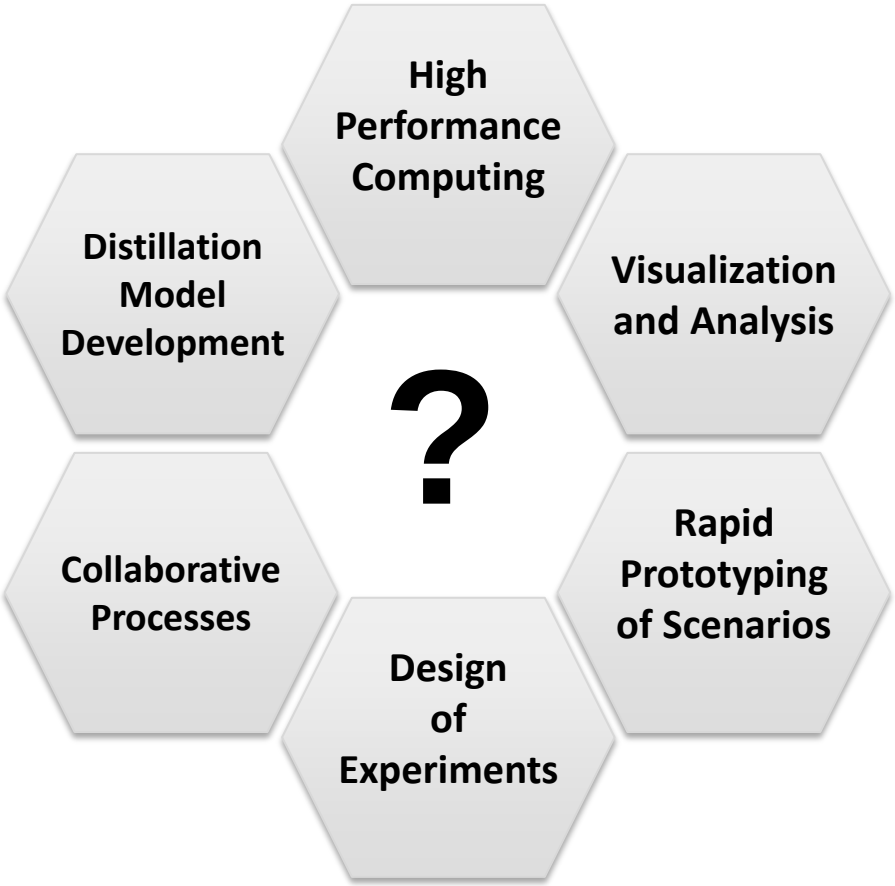
- NATO M&S Task Group 088 that codified the Data Farming process has been completed
- NATO M&S Task Group 124 (tasked with the application of Data Farming) is in progress

Data Farming Summary

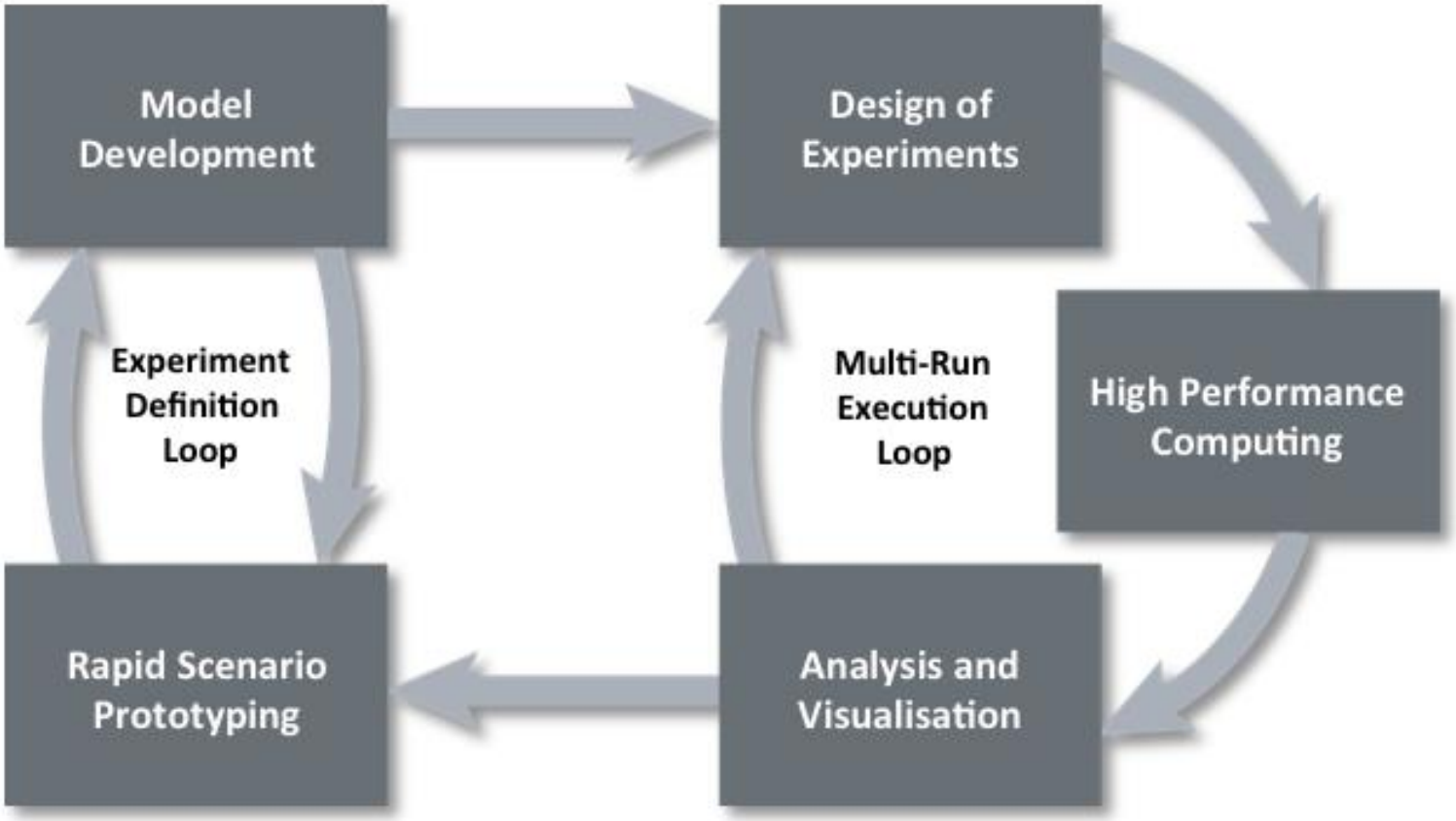
Data Farming **allows for the understanding of huge landscapes of possibilities and discovering outliers via the following realms or domains:**

- **Distillation Model Development**
- **High Performance Computing**
- **Data Visualization and Analysis**
- **Rapid Prototyping of Scenarios**
- **Design of Experiments**
- **Collaborative Processes**

Data Farming Domains



The Data Farming Loop of Loops



PAST DATA FARMING WORKSHOPS

PAIW, August 1999, Maui
PAIW 2, January 2000, Maui
PAIW 3, February 2001, Auckland
PAIW 4, August 2001, Australia
PAIW 5, July 2002, Germany
PAIW 6, March 2003, Monterey
PAIW 7, September 2003, Quantico
PAIW 8, April 2004, Singapore
PAIW 9, November 2004, Wellington
PAIW 10, May 2005, Stockholm
PAIW 11, February 2006, Honolulu
PAIW 12, June 2006, Germany

IDFW 13, November 2006, Netherlands
IDFW 14, March 2007, Monterey
IDFW 15, November 2007, Singapore
IDFW 16, March 2008, Monterey
IDFW 17, September 2008, Germany
IDFW 18, March 2009, Monterey
IDFW 19, November 2009, Auckland
IDFW 20, March 2010, Monterey
IDFW 21, September 2010, Portugal
IDFW 22, March 2011, Monterey
IDFW 23, September 2011, Finland
IDFW 24, March 2012, Monterey
IDFW 25, September 2012, Istanbul

IWW 26, June 2013, Washington
IWW 27, January 2014, Finland
IWW 28, October 2014, Washington
IWW 29, March 2015, Finland

Case Studies and Applications

MSG-088

- **Humanitarian Assistance/ Disaster Relief**
- **Force Protection**

MSG-124

- **Cyber Defense**
- **Operation Planning**

MSG-124 Cyber Syndicate Goals

- The overall objective of the task group is to apply data farming capabilities to contribute to the development of improved decision support to NATO forces.
- The overall goal of this syndicate is to provide quantitative insight into cyber security technologies and measures, for the purpose of providing more secure networks to NATO and partner nations.
- The team has developed a prototype simulation using an agent-based model and has begun to apply the data farming process to contribute to the development of improved decision support.

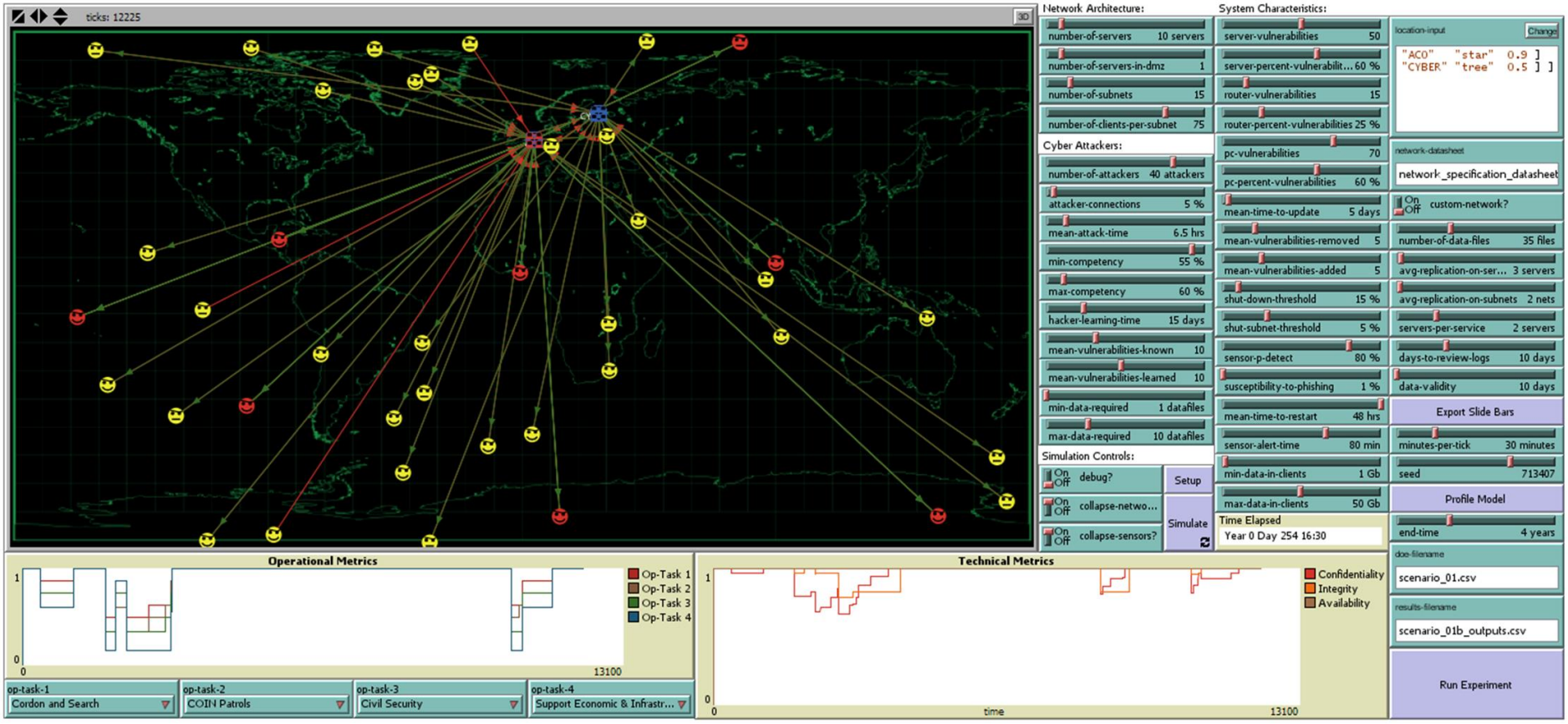
MSG-124 is applying data farming to Cyber Defense to contribute to improved decision support. Here are some questions that Data Farming may help solve:

- Canada: Is active defence more effective than passive defence?
- Australia: How do we assess the impact of different vulnerabilities?
- Turkey:. What is the impact of network vulnerability to the operational effectiveness of NATO forces?
- Sweden: How can cyber attacks be used to deceive the enemy? How can we manipulate the red side's view of the blue side's intention?
- US: How can we develop useful models of cyber space? Including models of the users, adversaries and defenders.
- Finland: How do legacy technologies impact the vulnerability of my network? How does the ability to defend the network change as it grows older?
- Italy: Can we identify synergies with research currently being conducted?
- Germany: How can we develop useful models of cyber space? How can we support other cyber groups with data farming?

Recent MSG-124 Cyber Syndicate Work

- Continued the model development process
- Set the base case model
- Using the base case, performed operations analysis through many iterations of the data farming process to begin to get insight into cyber security what-if? questions

Base Case Scenario



One question area explored :
What is the importance of the speed of patching?

1) Effectiveness of ‘Search and Attack’
2) Effectiveness of `Cordon Search’
3) Effectiveness of `Civil Security’
4) Effectiveness of `Support Economic and Infrastructure’

Data Farming Details

- DOE with 26 design points
- 312 total runs (12 replications for each design point)
- Parameters varied
  - Mean time to update (5 to 35 days)
  - Susceptibility to phishing (1% to 6%)
  - Maximum competency of attacker (60% to 90%)
  - Sensor probability of detection (30% to 80%)

Important Parameters
Effectiveness of 'Search and Attack'

Contrasts

Term	Contrast		Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
mean-time-to-update	-0.010593		-2.08	0.0419*	0.9999
susceptibility-to-phishing	-0.003274		-0.64	0.5268	1.0000
max-competency	-0.002311		-0.45	0.6582	1.0000
sensor-p-detect	0.000000		0.00	1.0000	1.0000
mean-time-to-update*mean-time-to-update	0.000267		0.05	0.9583	1.0000
mean-time-to-update*susceptibility-to-phishing	-0.001430		-0.28	0.7780	1.0000
susceptibility-to-phishing*susceptibility-to-phishing	0.000125	*	0.02	0.9813	1.0000
mean-time-to-update*max-competency	0.002247		0.44	0.6658	1.0000
susceptibility-to-phishing*max-competency	0.005924		1.16	0.2498	1.0000
max-competency*max-competency	-0.006289	*	-1.23	0.2225	1.0000
mean-time-to-update*sensor-p-detect	-0.001430		-0.28	0.7780	1.0000
susceptibility-to-phishing*sensor-p-detect	-0.001839		-0.36	0.7222	1.0000
max-competency*sensor-p-detect	-0.005516		-1.08	0.2822	1.0000
sensor-p-detect*sensor-p-detect	-0.006756	*	-1.32	0.1907	1.0000
mean-time-to-update*mean-time-to-update*susceptibility-to-phishing	-0.001158	*	-0.23	0.8253	1.0000
mean-time-to-update*susceptibility-to-phishing*susceptibility-to-phishing	-0.003745	*	-0.73	0.4684	1.0000
mean-time-to-update*mean-time-to-update*max-competency	0.007150	*	1.40	0.1667	1.0000
mean-time-to-update*susceptibility-to-phishing*max-competency	0.007967		1.56	0.1213	1.0000
mean-time-to-update*mean-time-to-update*sensor-p-detect	-0.010419	*	-2.04	0.0446*	0.9999
mean-time-to-update*susceptibility-to-phishing*sensor-p-detect	0.000204		0.04	0.9686	1.0000
mean-time-to-update*max-competency*sensor-p-detect	-0.003473		-0.68	0.5016	1.0000
susceptibility-to-phishing*max-competency*sensor-p-detect	0.000204		0.04	0.9686	1.0000
mean-time-to-update*susceptibility-to-phishing*max-competency*sensor-p-detect	0.002247		0.44	0.6658	1.0000

Important Parameters
Effectiveness of `Cordon Search'

Contrasts

Term	Contrast		Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
mean-time-to-update	-0.010497		-2.04	0.0418*	1.0000
susceptibility-to-phishing	-0.002600		-0.51	0.6091	1.0000
max-competency	-0.002022		-0.39	0.6882	1.0000
sensor-p-detect	0.000482		0.09	0.9237	1.0000
mean-time-to-update*mean-time-to-update	0.000614		0.12	0.9026	1.0000
mean-time-to-update*susceptibility-to-phishing	-0.001736		-0.34	0.7312	1.0000
susceptibility-to-phishing*susceptibility-to-phishing	0.000288	*	0.06	0.9547	1.0000
mean-time-to-update*max-competency	0.001532		0.30	0.7629	1.0000
susceptibility-to-phishing*max-competency	0.005822		1.13	0.2578	1.0000
max-competency*max-competency	-0.006181	*	-1.20	0.2276	1.0000
mean-time-to-update*sensor-p-detect	-0.001736		-0.34	0.7312	1.0000
susceptibility-to-phishing*sensor-p-detect	-0.001532		-0.30	0.7629	1.0000
max-competency*sensor-p-detect	-0.004801		-0.93	0.3491	1.0000
sensor-p-detect*sensor-p-detect	-0.006165	*	-1.20	0.2290	1.0000
mean-time-to-update*mean-time-to-update*susceptibility-to-phishing	-0.000919	*	-0.18	0.8558	1.0000
mean-time-to-update*susceptibility-to-phishing*susceptibility-to-phishing	-0.003711	*	-0.72	0.4708	1.0000
mean-time-to-update*mean-time-to-update*max-competency	0.007252	*	1.41	0.1564	1.0000
mean-time-to-update*susceptibility-to-phishing*max-competency	0.006844		1.33	0.1828	1.0000
mean-time-to-update*mean-time-to-update*sensor-p-detect	-0.009636	*	-1.88	0.0616	1.0000
mean-time-to-update*susceptibility-to-phishing*sensor-p-detect	-0.000511		-0.10	0.9183	1.0000
mean-time-to-update*max-competency*sensor-p-detect	-0.003779		-0.74	0.4633	1.0000
susceptibility-to-phishing*max-competency*sensor-p-detect	0.000511		0.10	0.9183	1.0000
mean-time-to-update*susceptibility-to-phishing*max-competency*sensor-p-detect	0.001532		0.30	0.7629	1.0000

Important Parameters
Effectiveness of `Civil Security'

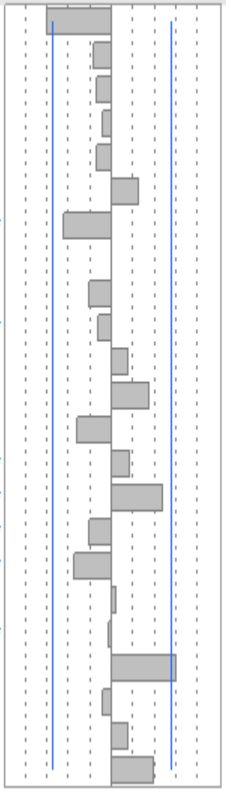
Contrasts

Term	Contrast		Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
mean-time-to-update	-0.011749		-2.06	0.0422*	0.9999
susceptibility-to-phishing	-0.002504		-0.44	0.6638	1.0000
max-competency	-0.001348		-0.24	0.8133	1.0000
sensor-p-detect	0.001156		0.20	0.8409	1.0000
mean-time-to-update*mean-time-to-update	-0.000614		-0.11	0.9128	1.0000
mean-time-to-update*susceptibility-to-phishing	-0.000613		-0.11	0.9130	1.0000
susceptibility-to-phishing*susceptibility-to-phishing	-0.000288	*	-0.05	0.9608	1.0000
mean-time-to-update*max-competency	0.003881		0.68	0.4937	1.0000
susceptibility-to-phishing*max-competency	0.007150		1.25	0.2073	1.0000
max-competency*max-competency	-0.008033	*	-1.41	0.1599	1.0000
mean-time-to-update*sensor-p-detect	0.000613		0.11	0.9130	1.0000
susceptibility-to-phishing*sensor-p-detect	-0.002656		-0.47	0.6421	1.0000
max-competency*sensor-p-detect	-0.004699		-0.82	0.4035	1.0000
sensor-p-detect*sensor-p-detect	-0.004490	*	-0.79	0.4251	1.0000
mean-time-to-update*mean-time-to-update*susceptibility-to-phishing	-0.000885	*	-0.16	0.8783	1.0000
mean-time-to-update*susceptibility-to-phishing*susceptibility-to-phishing	-0.004154	*	-0.73	0.4622	1.0000
mean-time-to-update*mean-time-to-update*max-competency	0.009329	*	1.64	0.1023	1.0000
mean-time-to-update*susceptibility-to-phishing*max-competency	0.009193		1.61	0.1068	1.0000
mean-time-to-update*mean-time-to-update*sensor-p-detect	-0.007559	*	-1.33	0.1837	1.0000
mean-time-to-update*susceptibility-to-phishing*sensor-p-detect	-0.000613		-0.11	0.9130	1.0000
mean-time-to-update*max-competency*sensor-p-detect	-0.002656		-0.47	0.6421	1.0000
susceptibility-to-phishing*max-competency*sensor-p-detect	0.000613		0.11	0.9130	1.0000
mean-time-to-update*susceptibility-to-phishing*max-competency*sensor-p-detect	0.002656		0.47	0.6421	1.0000

Important Parameters
Effectiveness of `Support Economic and Infrastructure'

Contrasts

Term	Contrast		Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
mean-time-to-update	-0.009052		-1.81	0.0706	1.0000
max-competency	-0.002504		-0.50	0.6176	1.0000
sensor-p-detect	-0.002022		-0.40	0.6854	1.0000
susceptibility-to-phishing	-0.001348		-0.27	0.7874	1.0000
mean-time-to-update*mean-time-to-update	-0.002017		-0.40	0.6860	1.0000
mean-time-to-update*max-competency	0.003677		0.73	0.4650	1.0000
max-competency*max-competency	-0.006814	*	-1.36	0.1767	1.0000
mean-time-to-update*sensor-p-detect	0.000000		0.00	1.0000	1.0000
max-competency*sensor-p-detect	-0.003064		-0.61	0.5457	1.0000
sensor-p-detect*sensor-p-detect	-0.001819	*	-0.36	0.7151	1.0000
mean-time-to-update*susceptibility-to-phishing	0.002247		0.45	0.6558	1.0000
max-competency*susceptibility-to-phishing	0.005311		1.06	0.2898	1.0000
sensor-p-detect*susceptibility-to-phishing	-0.004903		-0.98	0.3287	1.0000
susceptibility-to-phishing*susceptibility-to-phishing	0.002466	*	0.49	0.6239	1.0000
mean-time-to-update*mean-time-to-update*max-competency	0.007082	*	1.41	0.1603	1.0000
mean-time-to-update*max-competency*max-competency	-0.003201	*	-0.64	0.5305	1.0000
mean-time-to-update*mean-time-to-update*sensor-p-detect	-0.005311	*	-1.06	0.2898	1.0000
mean-time-to-update*max-competency*sensor-p-detect	0.000613		0.12	0.8995	1.0000
mean-time-to-update*mean-time-to-update*susceptibility-to-phishing	-0.000477	*	-0.10	0.9227	1.0000
mean-time-to-update*max-competency*susceptibility-to-phishing	0.008989		1.80	0.0728	1.0000
mean-time-to-update*sensor-p-detect*susceptibility-to-phishing	-0.001226		-0.24	0.8072	1.0000
max-competency*sensor-p-detect*susceptibility-to-phishing	0.002247		0.45	0.6558	1.0000
mean-time-to-update*max-competency*sensor-p-detect*susceptibility-to-phishing	0.005924		1.18	0.2384	1.0000



DATA FARMING WORKSHOPS

PAIW, August 1999, Maui
PAIW 2, January 2000, Maui
PAIW 3, February 2001, Auckland
PAIW 4, August 2001, Australia
PAIW 5, July 2002, Germany
PAIW 6, March 2003, Monterey
PAIW 7, September 2003, Quantico
PAIW 8, April 2004, Singapore
PAIW 9, November 2004, Wellington
PAIW 10, May 2005, Stockholm
PAIW 11, February 2006, Honolulu
PAIW 12, June 2006, Germany

IDFW 13, November 2006, Netherlands
IDFW 14, March 2007, Monterey
IDFW 15, November 2007, Singapore
IDFW 16, March 2008, Monterey
IDFW 17, September 2008, Germany
IDFW 18, March 2009, Monterey
IDFW 19, November 2009, Auckland
IDFW 20, March 2010, Monterey
IDFW 21, September 2010, Portugal
IDFW 22, March 2011, Monterey
IDFW 23, September 2011, Finland
IDFW 24, March 2012, Monterey
IDFW 25, September 2012, Istanbul

IWW 26, June 2013, Washington
IWW 27, January 2014, Finland
IWW 28, October 2014, Washington
IWW 29, March 2015, Finland

YOU ARE INVITED!

IWW 30, February 2016, Italy

IWW 31, October 2016, Finland