UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/947,575	09/22/2004	Jeremy Donald Kelley	END920040012US1	1294

47121 7590 01/24/2013

(SAUL-END) PATENT DOCKETING CLERK
IBM Corporation (SAUL-END) C/O Saul Ewing LLP
Penn National Insurance Tower
2 North Second Street, 7th Floor
Harrisburg, PA 17101

EXAMINER	
PAN, PEILIANG	
ART UNIT	**PAPER NUMBER**
2492	

NOTIFICATION DATE	DELIVERY MODE
01/24/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@saul.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JEREMY DONALD KELLEY, JEFFREY SCOTT LAHANN, and DAVID HUGH MACKEY II

Appeal 2010-007014
Application 10/947,575
Technology Center 2400

Before JOHN A. JEFFERY, BARBARA A. BENOIT, and JENNIFER L. McKEOWN, *Administrative Patent Judges*.

BENOIT, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the rejection of claims 1-21. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellants' invention relates to providing information about possible threats to information technology (IT) environments, including non-traditional IT threats. *See generally* Abstract. Claim 1 is representative and reads as follows, with key disputed limitations emphasized:

1. A computer-implemented method of rating a threat to the proper operation of an Information Technology (IT) system operated by an individual or organization, comprising the steps of:

collecting intelligence regarding *non-traditional IT threats to said IT system* in a non-traditional IT threat database;

analyzing said collected non-traditional IT threat intelligence using a computer processor configured to develop an overall threat score for each non-traditional IT threat that defines the overall potential for the non-traditional threat to do harm;

distributing said overall threat score, via a computer network, to said individual or organization; and

safeguarding said IT system based on said overall threat score.

The Examiner relies on the following as evidence of unpatentability:

Beavers	US 2003/0221123 A1	Nov. 27, 2003
Hnatio	US 2005/0004823 A1	Jan. 6, 2005 (filed Oct. 28, 2003)
Chung	US 7,187,279 B2	Mar. 6, 2007 (PCT pub. Sept. 10, 2004)

The Rejections

1. The Examiner rejected claims 1-5, 8-12, and 15-19 under 35 U.S.C. § 103(a) as unpatentable over Beavers and Hnatio. Ans. 4-6.[1]

2. The Examiner rejected claims 6, 7[2], 13, 14, 20, and 21 under 35 U.S.C. § 103(a) as unpatentable over Beavers, Hnatio, and Chung. Ans. 6-8.

CONTENTIONS

The Examiner finds that Beavers teaches every recited feature of illustrative claim 1 except for a non-traditional IT threat. Ans. 4-5. For this feature, the Examiner cites Hnatio in concluding that the claim would have been obvious to an ordinarily skilled artisan. Ans. 5 (citing Hnatio, Abstract, ¶ 0015).

Appellants argue that Hnatio teaches traditional terrorist threats affecting a general population, and so does not teach or suggest non-traditional IT threats as defined by Appellants' Specification. Br. 7-10. Appellants also contend that combining Beavers and Hnatio is improper and based on impermissible hindsight because there is nothing that would lead an ordinarily skilled artisan to combine Hnatio's detection of traditional

---

[1] Throughout this opinion, we refer to the Appeal Brief filed October 15, 2009 (Br.) and the Examiner's Answer mailed January 5, 2010 (Ans.).

[2] Claims 7, 14, and 21, which depend from claims 6, 13, and 20 respectively, are rejected under § 103 over Beavers, Hnatio, and Chung. Ans. 6. The Examiner, however, erroneously includes claims 7, 14, and 21 in the rejection over Beavers and Hnatio. *See* Ans. 4, 6. We deem this error harmless because the rejection of claims 7, 14, and 21 rely on the disclosure of Beaver, which is included in the rejection of claims 6, 13, and 20. Based on the record before us, we presume the Examiner intended to reject claims 7, 14, and 21 as being unpatentable over Beavers, Hnatio, and Chung and present the correct claim listing here for clarity.

terrorist threats and the detection of IT threats disclosed in Beavers. Br. 10-12.

ISSUES

1. Under § 103, has the Examiner erred in rejecting the claims by finding that Beavers and Hnatio collectively would have taught or suggested a non-traditional IT threat?

2. Under § 103, is the Examiner's reason to combine the teachings of Beavers and Hnatio supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

ANALYSIS

Obviousness Rejection of Claims 1-5, 8-12, and 15-19 over Beavers and Hnatio

Appellants do not dispute the Examiner's finding that Beavers teaches or suggests every step recited in claim 1 for a traditional IT threat. Br. 7-10. Nor do Appellants dispute that Hnatio teaches techniques for detecting terrorist attacks. Br. 8, 9. Rather, Appellants argue that Hnatio does not teach or suggest a non-traditional IT threat as defined by Appellants' Specification. Br. 8-10.

This appeal turns on whether it would have been obvious to extend Beavers techniques to non-traditional IT threats as disclosed by Hnatio. We therefore begin by determining whether the term "non-traditional IT threat" recited in claim 1 encompasses a terrorist threat.

As noted by Appellants (Br. 7-8), their Specification defines "non-traditional IT threats" as "threats that do not directly target computer systems and/or networks or that do not target anything at all, but that still

pose a threat to proper operation of the computer system or network." Spec. ¶ 0009. The Specification provides examples of non-traditional IT threats:

> Examples of non-traditional threats in the context of the present invention include, but are not limited to, weather-related problems (flooding, electrical storms, severe temperatures); atmospheric conditions affecting electrical devices such as sunspots and solar flares; *terrorist attacks on facilities in which networks are physically located or on electrical sources powering the networks*, and the like. For example, a hurricane or other weather-related event that could pose a great danger to the IT system of an organization (but which is not a specific IT threat) is not even considered in prior art threat analysis systems.

Id. (emphasis added). Notably, Appellants' Specification includes terrorist attacks as an example of non-traditional IT threats. *See also* Spec. ¶ 0018 (noting "non-traditional threats such as a terrorist or other physical attack on system hardware and facilities . . . are general in nature and may impact everything in their vicinity, including any network systems that may be in place."); ¶ 0019 (discussing terrorist attacks in September 2001 as an example of an attack that was not directed to network systems but nonetheless destroyed numerous network systems).

In light of the Appellants' Specification definition of non-traditional IT threats and explicit use of terrorist attacks as examples of non-traditional IT threats, we conclude non-traditional IT threats encompass terrorist attacks. Thus, we also do not perceive error in the Examiner's reliance on Hnatio's disclosure regarding terrorist attacks as teaching or suggesting non-traditional IT threats.

Turning now to whether the Examiner erred in concluding it would have been obvious to extend Beavers' techniques to include Hnatio's non-traditional IT threats, the Examiner explains that an ordinarily skilled artisan

would have been motivated to combine Beavers' system for dealing with threat severity with Hnatio's threat event analysis techniques to enhance Beavers' system. Ans. 5. Notably, as Appellants acknowledge (Br. 10), Hnatio describes attacks on computer systems and, in particular, describes cyber attacks on critical infrastructure as a "complex *non-traditional threats* to national security." Hnatio, ¶ 0015 (emphasis added); *see* Ans. 5 (citing Hnatio, ¶ 0015). The Examiner's combination of the teachings of Beavers and Hnatio is supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

We are not persuaded by Appellants' contention that Hnatio's teaching cannot be combined with Beavers' non-traditional IT threat because Hnatio merely teaches terrorism as a traditional threat in the realm of national security and so is not a non-traditional threat in an IT environment. Br. 10-11. As noted previously, Appellants' Specification uses terrorism as an example of a non-traditional IT threat, and Hnatio recognizes cyber attacks on critical infrastructure as a complex *non-traditional threat* to national security. Hnatio, ¶ 0015. The test for obviousness is what the references, when considered together, would suggest to an ordinarily skilled artisan, (*see In re Keller*, 642 F.2d 413, 425 (CCPA 1981)), who is a person of ordinary creativity and not an automaton, and whose inferences and creative steps may be considered, *KSR*, 550 U.S. at 417-18.

For the foregoing reasons, Appellants have not persuaded us of error in the Examiner's rejection of representative claim 1. We therefore will sustain the rejection of claim 1 and claims 2-5, 8-12, and 15-19, which were not separately argued with particularly.

Obviousness Rejection of Claims 6, 7, 13, 14, 20, and 21 over Beavers, Hnatio, and Chung

In challenging the obviousness rejection of claims 6, 13, and 20, Appellants rely on the same arguments with respect to the alleged deficiencies of the combination of Beavers and Hnatio in connection with independent claims 1, 8, and 15, from which claims 6, 13, and 20 respectively depend. Br. 12-13. Appellants also argue that Chung does not remedy those alleged deficiencies. Br. 13. We are not persuaded by these arguments, however, for the same reasons previously discussed. Claims 7, 14, and 21 were not argued separately with particularity. Br. 12.

Therefore, the rejection of claims 6, 7, 13, 14, 20, and 21 is sustained.

CONCLUSION

The Examiner did not err in rejecting claims 1-21 under § 103.

ORDER

The Examiner's decision rejecting claims 1-21 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

gvw